JOURNAL OF ALGEBRA 24, 258–282 (1973)

An Integral Basis Theorem for Jordan Algebras*

S. ROBERT GORDON

Department of Mathematics, University of California, Riverside, California 92502

Communicated by N. Jacobson

Received August 10, 1971

Let $\mathfrak{J}$ be a semisimple Jordan algebra, finite dimensional over an algebraically closed field of characteristic zero, and let $\mathfrak{K}$ be the Koecher–Tits algebra of $\mathfrak{J}$. In this paper it is shown that a Chevalley basis of $\mathfrak{K}$ can be chosen in such a way that those basis elements belonging to $\mathfrak{J}$ form an integral basis of $\mathfrak{J}$ regarded as a quadratic Jordan algebra. If we interpret the structure constants of $\mathfrak{J}$ and $\mathfrak{K}$ (with respect to these bases) over an arbitrary field F of characteristic $p \neq 2$, we obtain corresponding Jordan and Lie algebras $\mathfrak{J}_F$, $\mathfrak{K}_F$ over F. Two proofs that $\mathfrak{J}_F$ is semisimple are given: In the first it is shown that the generic trace of $\mathfrak{J}$ remains nondegenerate upon reduction modulo p, and in the second that $\mathfrak{K}_F/\mathfrak{Z}$ is isomorphic to the Koecher–Tits algebra of $\mathfrak{J}_F$ (here $\mathfrak{Z}$ is the center of $\mathfrak{K}_F$). It is also shown that $\mathfrak{J}_F$ is simple when $\mathfrak{J}$ is and that if F is algebraically closed then all semisimple Jordan algebras over F arise via this construction.

1. PRELIMINARIES

Throughout this paper $\mathfrak{J}$ is a finite dimensional semisimple Jordan algebra over an algebraically closed field Φ of characteristic zero (which may be taken to be the complex numbers). The product of $x, y \in \mathfrak{J}$ will be denoted by $x \cdot y$ and the regular representation of $\mathfrak{J}$ by $R_x : y \to x \cdot y$. The quadratic representation of $\mathfrak{J}$ is $U_x = 2R_x^2 - R_{x^2}$. The various Lie algebras associated with $\mathfrak{J}$ are the derivation algebra $\mathfrak{D} = [R_\mathfrak{J}, R_\mathfrak{J}]$, the structure Lie algebra $\mathfrak{L} = R_\mathfrak{J} \oplus \mathfrak{D}$, and the Koecher–Tits algebra $\mathfrak{K} = \mathfrak{J} \oplus \bar{\mathfrak{J}} \oplus \mathfrak{L}$. The definitions and elementary properties of these algebras are given in [5], especially in Chapter VIII, and are summarized in [2, pp. 3, 4]. $\mathfrak{K}$ is a semisimple Lie algebra over Φ, and thus has the usual Cartan decomposition as a direct sum of a Cartan subalgebra and the associated root spaces. In this

* This research was supported in part by NSF Grant GP-9661.

paper we shall make elaborate use of the particular Cartan decomposition studied in [2]. Briefly, this decomposition arises as follows: Let $\mathfrak{W}$ be a fixed, arbitrary Cartan subalgebra of $\mathfrak{D}$, $\mathfrak{A} = \{x \in \mathfrak{J} \mid x\mathfrak{W} = 0\}$. Then $\mathfrak{H} = R_{\mathfrak{A}} + \mathfrak{W}$ is the unique Cartan subalgebra of $\mathfrak{R}$ containing $\mathfrak{W}$ [2, Proposition 1]. The root space $\mathfrak{R}_\rho$ of any root ρ relative to $\mathfrak{H}$ is contained either in $\mathfrak{J}$, $\bar{\mathfrak{J}}$, or $\mathfrak{L}' = [\mathfrak{L}, \mathfrak{L}]$; $\mathfrak{H}_1 = \mathfrak{H} \cap \mathfrak{L}'$ is a Cartan subalgebra of $\mathfrak{L}'$ and one has a natural bijection $\alpha \mapsto \hat{\alpha}$ from the roots of $\mathfrak{L}'$ (relative to $\mathfrak{H}_1$) to the roots of $\mathfrak{R}$ (relative to $\mathfrak{H}$) whose root spaces are contained in $\mathfrak{L}'$ [2, p. 6 and Proposition 6]. If ϵ is the automorphism of $\mathfrak{R}$ which sends $a + \bar{b} + R_c + D \to b + \bar{a} - R_c + D$ ($a, b, c \in \mathfrak{J}$; $D \in \mathfrak{D}$) then ϵ stabilizes $\mathfrak{H}$ and $\mathfrak{H}_1$, so ϵ^* acts on the roots of $\mathfrak{R}$ and $\mathfrak{L}'$ [2, pp. 4 and 6]. One can choose a simple system $\{\alpha_1, \ldots, \alpha_l\}$ of roots of $\mathfrak{L}'$ stabilized by ϵ^* [2, Proposition 15]. Given such a simple system, there are unique roots $\rho_1, \ldots, \rho_r$ of $\mathfrak{R}$ such that $\mathfrak{R}_{\rho_i} \subseteq \mathfrak{J}$ and $\{\rho_1, \ldots, \rho_r, \hat{\alpha}_1, \ldots, \hat{\alpha}_l\}$ is a simple system of roots of $\mathfrak{R}$ [2, Proposition 9]. We choose and fix such a simple system.

The following facts about $\mathfrak{A}$ will be needed. Since $\mathfrak{A} \subseteq \mathfrak{J}$, we can regard $\mathfrak{A}$ as a subspace of $\mathfrak{R}$. Then $\mathfrak{A} = \bigoplus \sum_{\rho \in P} \mathfrak{R}_\rho$, where P is the set of roots ρ of $\mathfrak{R}$ such that $\mathfrak{R}_\rho \subseteq \mathfrak{J}$, $\rho(\mathfrak{W}) = 0$, and is also the set of roots ρ such that $\mathfrak{R}_\rho \subseteq \mathfrak{J}$, $\rho\epsilon^* = -\rho$ [2, pp. 12, 13]. Since $1 \in \mathfrak{A}$, we can write $1 = \sum_{\rho \in P} e_\rho$, where $e_\rho \in \mathfrak{R}_\rho$; then $\{e_\rho \mid \rho \in P\}$ is a set of (nonzero) orthogonal idempotents of $\mathfrak{J}$ [2, Proposition 13].

2. An Integral Basis of $\mathfrak{R}$

Our first business is to show how the simple ideals of $\mathfrak{J}$ may be recovered from the Cartan decomposition of $\mathfrak{R}$. $\mathfrak{J}$ is the direct sum of root spaces $\mathfrak{R}_{\rho_i + \hat{\alpha}}$, where $\alpha \in \mathfrak{H}_1{}^*$ [2, Proposition 8]. For each $i = 1, \ldots, r$ let $\mathfrak{J}_i$ be the sum of all root spaces $\mathfrak{R}_{\rho_i + \hat{\alpha}}$; then $\mathfrak{J} = \mathfrak{J}_1 \oplus \cdots \oplus \mathfrak{J}_r$.

Lemma 1. *Each $\mathfrak{J}_i$ is an ideal of $\mathfrak{J}$.*

Proof. Suppose x is a root vector for $\rho_i + \hat{\alpha}$ (i.e., $x \in \mathfrak{R}_{\rho_i + \hat{\alpha}}$), y for $\rho_j + \hat{\beta}$, and suppose $i \neq j$. Then $\bar{y}$ is a root vector for $(\rho_j + \hat{\beta})\,\epsilon^* = -\rho_j + \hat{\gamma}$ (for some $\gamma \in \mathfrak{H}_1{}^*$: see [2, Proposition 14]). Since $\rho_i - \rho_j + \hat{\alpha} + \hat{\gamma}$ is not a root [2, Proposition 8] we must have $[x, \bar{y}] = 0$. But $[x, \bar{y}] = 2(R_{x \cdot y} - [R_x, R_y])$, so that $x \cdot y = 0$, $[R_x, R_y] = 0$. By linearity we see that $\mathfrak{J}_i \cdot \mathfrak{J}_j = 0$ and $[R_{\mathfrak{J}_i}, R_{\mathfrak{J}_j}] = 0$.

Now for $x \in \mathfrak{J}$ let $x = \sum_{i=1}^r x_i$ where $x_i \in \mathfrak{J}_i$. In particular, if $1 = \sum_i 1_i$ then $x_i = 1 \cdot x_i = \sum_j 1_j \cdot x_i = 1_i \cdot x_i$. So if $x \in \mathfrak{J}$, then

$$1_i \cdot x = \sum_j 1_i \cdot x_j = 1_i \cdot x_i = x_i .$$

Finally if $x \in \mathfrak{J}$, $y \in \mathfrak{J}_i$, and $j \neq i$ then $0 = [R_{1_j}, R_y]$; so

$$0 = [1_j, x, y] = (1_j \cdot x) \cdot y - 1_j \cdot (x \cdot y) = x_j \cdot y - (x \cdot y)_j = 0 - (x \cdot y)_j .$$

I.e. $(x \cdot y)_j = 0$ for all $j \neq i$ and thus $x \cdot y \in \mathfrak{J}_i$. This completes the proof.

Now $\mathfrak{J}_i \neq 0$ since, for example, $\mathfrak{R}_{\rho_i} \subseteq \mathfrak{J}_i$. So the number s of simple summands of $\mathfrak{J}$ is at least r : $s \geqslant r$. On the other hand, suppose $\mathfrak{J} = \mathfrak{J}_1' \oplus \cdots \oplus \mathfrak{J}_s'$ is the decomposition of $\mathfrak{J}$ as a sum of simple ideals and let c_i be the identity of $\mathfrak{J}_i'$. Then $R_{c_1}, ..., R_{c_s}$ are linearly independent elements of $\mathfrak{R}$ and clearly belong to the center $\mathfrak{C}$ of $\mathfrak{L}$ (since $[R_{c_i}, R_x] = 0$ for all $x \in \mathfrak{J}$). But $r = \dim \mathfrak{H}^* - \dim \mathfrak{H}_1{}^* = \dim \mathfrak{H} - \dim \mathfrak{H}_1 = \dim \mathfrak{C}$ [2, p. 4]. So $s \leqslant r$. We conclude that $s = r$ and that each $\mathfrak{J}_i$ is simple. It is also clear that if 1_i is as in the proof of Lemma 1, then 1_i is the identity of $\mathfrak{J}_i$.

Suppose ρ, τ are roots of $\mathfrak{R}$ such that $\rho, \tau \in P$, $\rho \neq \tau$, and $\mathfrak{R}_\rho, \mathfrak{R}_\tau \subseteq \mathfrak{J}_i$ for some i. Then e_ρ, e_τ are orthogonal idempotents belonging to $\mathfrak{J}_i$. We claim that the intersection of the Peirce half-spaces $\mathfrak{J}_{1/2}(e_\rho) \cap \mathfrak{J}_{1/2}(e_\tau)$ is not zero. Indeed, $1_i = (1_i - e_\rho - e_\tau) + e_\rho + e_\tau$ is a decomposition of 1_i as a sum of orthogonal idempotents. This decomposition can be refined to a decomposition of 1_i as a sum of primitive orthogonal idempotents. Since Φ is algebraically closed, these idempotents are absolutely primitive [5, p. 197]. Let e be a primitive idempotent occurring in the decomposition of e_ρ and f a primitive idempotent occurring in the decomposition of e_τ. The simplicity of $\mathfrak{J}_i$ together with the usual argument about reduced Jordan algebras [5, pp. 179, 180, 202] shows that e and f are connected, i.e., $\mathfrak{J}_{1/2}(e) \cap \mathfrak{J}_{1/2}(f) \neq 0$. Certainly, $\mathfrak{J}_{1/2}(e) \cap \mathfrak{J}_{1/2}(f) \subseteq \mathfrak{J}_{1/2}(e_\rho) \cap \mathfrak{J}_{1/2}(e_\tau)$.

We will write the Peirce decomposition of $\mathfrak{J}$ with respect to the idempotents e_ρ ($\rho \in P$) as $\mathfrak{J} = \oplus \sum_{\rho,\tau \in P} \mathfrak{J}_{\rho\tau}$. We have just shown that if $\mathfrak{R}_\rho$, $\mathfrak{R}_\tau \subseteq \mathfrak{J}_i$ then $\mathfrak{J}_{\rho\tau} \neq 0$.

For $\rho, \tau \in P$ we claim that $\mathfrak{J}_{\rho\tau}$ is a direct sum of root spaces of $\mathfrak{R}$. For this it is sufficient to show that $[\mathfrak{J}_{\rho\tau}, \mathfrak{H}] \subseteq \mathfrak{J}_{\rho\tau}$. Suppose $\rho \in P$, $x \in \mathfrak{J}$, and $R_a + D \in \mathfrak{H}$. Then $a \in \mathfrak{A}$ and so $[R_{e\rho}, R_a] = 0$. Also $D \in \mathfrak{W}$ so that $(e_\rho \cdot x)\, D = (e_\rho D) \cdot x + e_\rho \cdot (xD) = e_\rho \cdot (xD)$, by the definition of $\mathfrak{A}$. Thus

$$\begin{aligned} e_\rho \cdot [x, R_a + D] &= e_\rho \cdot (x \cdot a + xD) = (e_\rho \cdot x) \cdot a + (e_\rho \cdot x)\, D \\ &= [e_\rho \cdot x, R_a + D]. \end{aligned}$$

So if $x \in \mathfrak{J}_\theta(e_\rho)$ (where $\theta = 0, \frac{1}{2}, 1$) then also $[x, R_a + D] \in \mathfrak{J}_\theta(e_\rho)$. Thus if $\rho \neq \tau$, $\mathfrak{J}_{\rho\rho} = \mathfrak{J}_1(e_\rho)$ and $\mathfrak{J}_{\rho\tau} = \mathfrak{J}_{1/2}(e_\rho) \cap \mathfrak{J}_{1/2}(e_\tau)$ are invariant under ad $\mathfrak{H}$.

Let τ be a root of $\mathfrak{R}$ such that $\mathfrak{R}_\tau \subseteq \mathfrak{J}$ and let $\rho \in P$. We claim that $\tau - \rho$ is a root if and only if $\mathfrak{R}_\tau \subseteq \mathfrak{J}_1(e_\rho) \oplus \mathfrak{J}_{1/2}(e_\rho)$. Indeed $\mathfrak{R}_\tau$ must be contained in one of $\mathfrak{J}_1(e_\rho)$, $\mathfrak{J}_{1/2}(e_\rho)$, $\mathfrak{J}_0(e_\rho)$ by the preceding paragraph. Since $\rho\epsilon^* = -\rho$, the root space of $-\rho$ is $\mathfrak{R}_\rho\epsilon = \Phi\bar{e}_\rho$. Thus $\tau - \rho$ is a root if and only if $[\mathfrak{R}_\tau, \bar{e}_\rho] \neq 0$. Let $x \in \mathfrak{R}_\tau$. If $x \in \mathfrak{J}_\theta(e_\rho)$, $\theta = 1$ or $\frac{1}{2}$, then

$$[x, \bar{e}_\rho] = 2(R_{x \cdot e_\rho} - [R_x, R_{e_\rho}]),$$

which is not zero since $x \cdot e_\rho = \theta x \neq 0$. On the other hand, if $x \in \mathfrak{J}_0(e_\rho)$ then certainly $x \cdot e_\rho = 0$. Also $[R_x, R_{e_\rho}] = 0$; for if y belongs to $\mathfrak{J}_1(e_\rho)$ or $\mathfrak{J}_0(e_\rho)$, then $(x \cdot y) \cdot e_\rho = x \cdot (y \cdot e_\rho) = 0$ and if $y \in \mathfrak{J}_{1/2}(e_\rho)$, then $[x, y, e_\rho] = 0$ by [5, p. 121, identity PD2]. Thus $[x, \bar{e}_\rho] = 0$ in this case.

Our principal lemma is the following:

LEMMA 2. *There exists an automorphism σ of $\mathfrak{R}$ with the following properties:*

(1) $H\sigma = -H$ *for all* $H \in \mathfrak{H}$;

(2) $\mathfrak{R}_\rho\sigma = \mathfrak{R}_{-\rho}$ *for all roots* ρ *of* $\mathfrak{R}$, *and* $\sigma^2 = 1$;

(3) σ *and* ϵ *commute;*

(4) $e_\rho\sigma = \bar{e}_\rho$ *for all* $\rho \in P$.

Proof. We recall that for any root ρ, $H_\rho \in \mathfrak{H}$ is defined to be that element of $[\mathfrak{R}_\rho, \mathfrak{R}_{-\rho}]$ such that $\rho(H_\rho) = 2$. If for each simple root ρ of $\mathfrak{R}$ we choose $E_\rho \in \mathfrak{R}_\rho$, $F_\rho \in \mathfrak{R}_{-\rho}$ so that $[E_\rho, F_\rho] = H_\rho$, then there is an automorphism of $\mathfrak{R}$ which sends $E_\rho \to F_\rho$, $F_\rho \to E_\rho$, $H_\rho \to -H_\rho$ [4, p. 127]. Such an automorphism satisfies properties (1) and (2) of the Lemma [4, p. 147]. The set of elements $\{E_\rho, F_\rho, H_\rho \mid \rho \text{ is a simple root}\}$ is called a canonical system of generators of $\mathfrak{R}$. Our aim is to choose these generators in such a way as to make the resulting automorphism satisfy (3) and (4).

We choose a canonical system of generators as follows:

(a) If α_i is a simple root of $\mathfrak{L}'$ such that $\alpha_i\epsilon^* = \alpha_i$, let $E_{\hat{\alpha}_i}$, $F_{\hat{\alpha}_i}$ be arbitrary elements of $\mathfrak{R}_{\hat{\alpha}_i}$, $\mathfrak{R}_{-\hat{\alpha}_i}$ (respectively) such that $[E_{\hat{\alpha}_i}, F_{\hat{\alpha}_i}] = H_{\hat{\alpha}_i}$.

(b) If α_i, α_j $(i < j)$ are simple roots of $\mathfrak{L}'$ such that $\alpha_i\epsilon^* = \alpha_j$, choose $E_{\hat{\alpha}_i} \in \mathfrak{R}_{\hat{\alpha}_i}$, $F_{\hat{\alpha}_i} \in \mathfrak{R}_{-\hat{\alpha}_i}$ such that $[E_{\hat{\alpha}_i}, F_{\hat{\alpha}_i}] = H_{\hat{\alpha}_i}$. Let $E_{\hat{\alpha}_j} = E_{\hat{\alpha}_i}\epsilon$, $F_{\hat{\alpha}_j} = F_{\hat{\alpha}_i}\epsilon$. Note that $\mathfrak{R}_{\hat{\alpha}_i}\epsilon = \mathfrak{R}_{\hat{\alpha}_j}$ and $\mathfrak{R}_{-\hat{\alpha}_i}\epsilon = \mathfrak{R}_{-\hat{\alpha}_j}$. Also

$$[E_{\hat{\alpha}_j}, [E_{\hat{\alpha}_j}, F_{\hat{\alpha}_j}]] = [E_{\hat{\alpha}_i}, [E_{\hat{\alpha}_i}, F_{\hat{\alpha}_i}]]\,\epsilon = 2E_{\hat{\alpha}_i}\epsilon = 2E_{\hat{\alpha}_j},$$

so that $[E_{\hat{\alpha}_j}, F_{\hat{\alpha}_j}] = H_{\hat{\alpha}_j}$.

(c) For $i = 1, \ldots, r$, choose $E_{\rho_i} \in \mathfrak{R}_{\rho_i}$, $F_{\rho_i} \in \mathfrak{R}_{-\rho_i}$ arbitrarily so that $[E_{\rho_i}, F_{\rho_i}] = H_{\rho_i}$.

Let σ be the automorphism of $\mathfrak{R}$ which sends $E_\rho \to F_\rho$ and $F_\rho \to E_\rho$ for all simple roots ρ, where E_ρ, F_ρ are as in (a), (b), and (c). We first note that $E_\rho\sigma\epsilon = E_\rho\epsilon\sigma$ and $F_\rho\sigma\epsilon = F_\rho\epsilon\sigma$ if $\rho = \hat{\alpha}_i$.

To see this, first suppose that α_i is as in (a). This means that $\mathfrak{R}_{\hat{\alpha}_i}$ is contained either in $R_{\mathfrak{Z}}$ or in $\mathfrak{D}$ [2, p. 20]. The same applies to $\mathfrak{R}_{-\hat{\alpha}_i}$. We claim that $\mathfrak{R}_{\hat{\alpha}_i} \subseteq \mathfrak{D}$ if and only if $\mathfrak{R}_{-\hat{\alpha}_i} \subseteq \mathfrak{D}$. Otherwise we have root vectors R_a and D of $\mathfrak{R}$ such that $H_{\hat{\alpha}_i} = \pm [R_a, D] = \pm R_{aD}$. Now if $\langle\,,\rangle$ is the Killing form of $\mathfrak{L}'$ then $\langle R_{aD}, \mathfrak{W}\rangle = 0$ [2, Proposition 3]. Thus for all $D' \in \mathfrak{W}$ we have

$$0 = \langle H_{\hat{\alpha}_i}, D'\rangle = \frac{2}{\langle \alpha_i, \alpha_i\rangle} \alpha_i(D')$$

by [4, p. 112], so that $\hat{\alpha}_i(D') = \alpha_i(D') = 0$. Since R_a is a root vector either for $\hat{\alpha}_i$ or for $-\hat{\alpha}_i$, we have $[R_a, D'] = 0$, i.e., $aD' = 0$. This means that $a\mathfrak{W} = 0$, i.e., $a \in \mathfrak{A}$, i.e. $R_a \in \mathfrak{H}$, a contradiction to the assumption that R_a is a root vector.

Since $\mathfrak{R}_{\hat{\alpha}_i} \subseteq \mathfrak{D}$ if and only if $\mathfrak{R}_{-\hat{\alpha}_i} \subseteq \mathfrak{D}$, we have $E_{\hat{\alpha}_i}\epsilon = \lambda E_{\hat{\alpha}_i}$ and $F_{\hat{\alpha}_i}\epsilon = \lambda F_{\hat{\alpha}_i}$, where $\lambda = \pm 1$. In either case,

$$E_{\hat{\alpha}_i}\epsilon\sigma = \lambda E_{\hat{\alpha}_i}\sigma = \lambda F_{\hat{\alpha}_i} = F_{\hat{\alpha}_i}\epsilon = E_{\hat{\alpha}_i}\sigma\epsilon,$$

$$F_{\hat{\alpha}_i}\epsilon\sigma = E_{\hat{\alpha}_i}\sigma\epsilon\sigma = E_{\hat{\alpha}_i}\epsilon\sigma\sigma = E_{\hat{\alpha}_i}\epsilon = F_{\hat{\alpha}_i}\sigma\epsilon.$$

Now suppose that α_i, α_j are as in (b). Then

$$E_{\hat{\alpha}_i}\epsilon\sigma = E_{\hat{\alpha}_j}\sigma = F_{\hat{\alpha}_j} = F_{\hat{\alpha}_i}\epsilon = E_{\hat{\alpha}_i}\sigma\epsilon,$$

$$E_{\hat{\alpha}_j}\epsilon\sigma = E_{\hat{\alpha}_i}\epsilon\epsilon\sigma = E_{\hat{\alpha}_i}\sigma = F_{\hat{\alpha}_i} = F_{\hat{\alpha}_i}\epsilon\epsilon = F_{\hat{\alpha}_j}\epsilon = E_{\hat{\alpha}_j}\sigma\epsilon.$$

And as in case (a) above

$$F_{\hat{\alpha}_i}\epsilon\sigma = F_{\hat{\alpha}_i}\sigma\epsilon \qquad \text{and} \qquad F_{\hat{\alpha}_j}\epsilon\sigma = F_{\hat{\alpha}_j}\sigma\epsilon.$$

We know that for $i = 1,\dots, r$, $\rho_i\epsilon^* = -\rho_i - \sum_{k=1}^{l} n_k\hat{\alpha}_k$ for some non-negative integers n_k [2, Proposition 14]. Since $E_{\rho_i}\epsilon \in \mathfrak{R}_{\rho_i\epsilon^*}$, it follows that $E_{\rho_i}\epsilon = \theta[[A, F_{\rho_i}], B]$, where $0 \neq \theta \in \Phi$ and A and B are (possibly vacuous) Lie monomials in $F_{\hat{\alpha}_1}, \dots, F_{\hat{\alpha}_l}$ [4, p. 123]. Now

$$[[A, F_{\rho_i}], B]\,\sigma = [[A\sigma, E_{\rho_i}], B\sigma] \in \mathfrak{R}_{\rho_i\epsilon^*}\sigma = \mathfrak{R}_{-\rho_i\epsilon^*}.$$

Hence since $F_{\rho_i}\epsilon \in \mathfrak{R}_{-\rho_i\epsilon^*}$ we must have

$$F_{\rho_i}\epsilon = \psi[[A\sigma, E_{\rho_i}], B\sigma]$$

for some $\psi \in \Phi$. We now choose a new canonical system of generators as follows: $E_{\hat{\alpha}_i}$ and $F_{\hat{\alpha}_i}$ are as in (a) and (b). And

(c′) For each $i = 1,\dots, r$ let α be a fourth root of ψ/θ and let $E'_{\rho_i} = \alpha E_{\rho_i}$ and $F'_{\rho_i} = \alpha^{-1}F_{\rho_i}$. Clearly $[E'_{\rho_i}, F'_{\rho_i}] = H_{\rho_i}$.

Let σ' be the automorphism of $\mathfrak{R}$ which interchanges $E_{\hat{\alpha}_i}, F_{\hat{\alpha}_i}$ and also interchanges E'_{ρ_i}, F'_{ρ_i}. We claim that σ' satisfies the first three properties of the Lemma. Since (c′) is a special case of (c) we have already shown that $E_{\hat{\alpha}_i}\epsilon\sigma' = E_{\hat{\alpha}_i}\sigma'\epsilon$ and $F_{\hat{\alpha}_i}\epsilon\sigma' = F_{\hat{\alpha}_i}\sigma'\epsilon$ for $i = 1,..., l$. In addition,

$$\begin{aligned} E'_{\rho_i}\epsilon\sigma' &= \alpha E_{\rho_i}\epsilon\sigma' = \alpha\theta[[A, F_{\rho_i}], B]\,\sigma' \\ &= \alpha^2\theta[[A, F'_{\rho_i}], B]\,\sigma' \\ &= \alpha^2\theta[[A\sigma', E'_{\rho_i}], B\sigma'] \\ &= \alpha^3\theta[[A\sigma, E_{\rho_i}], B\sigma] \\ &= \alpha^3\theta\psi^{-1}F_{\rho_i}\epsilon = \alpha^4\theta\psi^{-1}F'_{\rho_i}\epsilon \\ &= \alpha^4\theta\psi^{-1}E'_{\rho_i}\sigma'\epsilon = E'_{\rho_i}\sigma'\epsilon. \end{aligned}$$

And, as before, this implies that $F'_{\rho_i}\epsilon\sigma' = F'_{\rho_i}\sigma'\epsilon$. Since the elements chosen in (a), (b), and (c′) generate $\mathfrak{R}$, we have $\sigma'\epsilon = \epsilon\sigma'$.

We claim that for each $\rho \in P$, $e_\rho\sigma' = \pm\bar{e}_\rho$. First note that since $\rho\epsilon^* = -\rho$, $\bar{e}_\rho \in \mathfrak{R}_{-\rho}$. Also

$$[e_\rho, \bar{e}_\rho] = 2(R_{e_\rho\cdot e_\rho} - [R_{e_\rho}, R_{e_\rho}]) = 2R_{e_\rho}$$

and

$$[e_\rho, 2R_{e_\rho}] = 2e_\rho \cdot e_\rho = 2e_\rho .$$

This means that $H_\rho = 2R_{e_\rho}$. If $\lambda e_\rho \in \mathfrak{R}_\rho$ is such that $[\lambda e_\rho, \lambda\bar{e}_\rho] = H_\rho$, then $\lambda^2 = 1$, i.e., $\lambda = \pm 1$. Finally $e_\rho\sigma'\epsilon \in \mathfrak{R}_\rho\sigma'\epsilon = \mathfrak{R}_{-\rho\epsilon^*} = \mathfrak{R}_\rho$ and

$$\begin{aligned} [e_\rho\sigma'\epsilon, \overline{e_\rho\sigma'\epsilon}] &= [e_\rho\sigma'\epsilon, e_\rho\sigma'] = [e_\rho\epsilon\sigma', e_\rho\sigma'] \\ &= [e_\rho\epsilon, e_\rho]\,\sigma' = [\bar{e}_\rho, e_\rho]\,\sigma' \\ &= (-H_\rho)\,\sigma' = H_\rho . \end{aligned}$$

This proves as desired that $e_\rho\sigma'\epsilon = \pm e_\rho$, i.e., $e_\rho\sigma' = \pm\bar{e}_\rho$.

It will next be shown that if $\rho, \tau \in P$ are such that $\mathfrak{R}_\rho, \mathfrak{R}_\tau$ are contained in the same simple summand of $\mathfrak{J}$, then $e_\rho\sigma'\epsilon = e_\rho$ if and only if $e_\tau\sigma'\epsilon = e_\tau$. Suppose, say, that $e_\rho\sigma'\epsilon = e_\rho$ and $e_\tau\sigma'\epsilon = -e_\tau$. Clearly $\rho \neq \tau$. Let ν be a root of $\mathfrak{R}$ such that $\mathfrak{R}_\nu \subseteq \mathfrak{J}_{\rho\tau}$. If $x \in \mathfrak{R}_\nu$, then

$$\begin{aligned} [e_\rho[e_\tau\bar{x}]] &= [e_\rho, 2(R_{e_\tau\cdot x} - [R_{e_\tau}, R_x])] \\ &= 2(e_\rho \cdot (e_\tau \cdot x) - (e_\rho \cdot e_\tau) \cdot x + (e_\rho \cdot x) \cdot e_\tau) \\ &= 2(\tfrac{1}{4}x - 0 + \tfrac{1}{4}x) = x. \end{aligned}$$

We have already observed that $\nu - \rho$ and $\nu - \tau$ are roots. So

$$(\nu - \rho)\,\sigma'^*\epsilon^* = \nu\sigma'^*\epsilon^* + \rho\epsilon^* = \nu\sigma'^*\epsilon^* - \rho$$

and

$$(\nu - \tau)\,\sigma'^*\epsilon^* = \nu\sigma'^*\epsilon^* - \tau$$

are both roots. Thus the root space of $\nu\sigma'^*\epsilon^*$ is contained in

$$(\mathfrak{J}_1(e_\rho) \oplus \mathfrak{J}_{1/2}(e_\rho)) \cap (\mathfrak{J}_1(e_\tau) \oplus \mathfrak{J}_{1/2}(e_\tau)) = \mathfrak{J}_{\rho\tau}$$

Since $x\sigma'\epsilon$ is a root vector for $\nu\sigma'^*\epsilon^*$ we conclude that

$$[e_\rho\,,\,[e_\tau\,,\,\overline{x\sigma'\epsilon}]] = x\sigma'\epsilon.$$

But then

$$\begin{aligned} x\sigma'\epsilon &= [e_\rho[e_\tau\bar{x}]]\,\sigma'\epsilon = [e_\rho\sigma'\epsilon,\,[e_\tau\sigma'\epsilon,\,\bar{x}\sigma'\epsilon]] \\ &= [e_\rho\,,\,[-e_\tau\,,\,x\epsilon\sigma'\epsilon]] = -\,[e_\rho\,,\,[e_\tau\,,\,x\sigma'\epsilon\epsilon]] \\ &= -\,[e_\rho\,,\,[e_\tau\,,\,\overline{x\sigma'\epsilon}]] = -x\sigma'\epsilon, \end{aligned}$$

a contradiction if $x \neq 0$.

We now choose a third canonical system of generators by replacing (c′) by

(c″) For each $i = 1,..., r$ let α be as chosen in (c′). If $\mathfrak{J}_i$ has the property that $e_\rho\sigma'\epsilon = e_\rho$ whenever $\rho \in P$, $e_\rho \in \mathfrak{J}_i$, let $E''_{\rho_i} = E'_{\rho_i} = \alpha E_{\rho_i}$ and $F''_{\rho_i} = F'_{\rho_i} = \alpha^{-1}F_{\rho_i}$. If $\mathfrak{J}_i$ has the property that $e_\rho\sigma'\epsilon = -e_\rho$ whenever $\rho \in P$, $e_\rho \in \mathfrak{J}_i$, let

$$E''_{\rho_i} = \sqrt{-1}\,E'_{\rho_i} = \sqrt{-1}\,\alpha E_{\rho_i}$$

and

$$F''_{\rho_i} = -\sqrt{-1}\,F'_{\rho_i} = -\sqrt{-1}\,\alpha^{-1}F_{\rho_i}\,.$$

(Note that for each i there is some $\rho \in P$ such that $e_\rho \in \mathfrak{J}_i$ [2, Proposition 13(b)].)

Certainly $[E''_{\rho_i}\,, F''_{\rho_i}] = H_{\rho_i}$ for $i = 1,..., r$. Let σ'' be the automorphism of $\mathfrak{R}$ which interchanges $E_{\hat\alpha_i}\,, F_{\hat\alpha_i}$ and also interchanges $E''_{\rho_i}\,, F''_{\rho_i}$. Since $\sqrt{-1}\,\alpha$ is also a fourth root of ψ/θ, (c'') is a special case of (c'). Hence the facts proven about σ' also apply to σ'' : σ'' commutes with ϵ, and for each $\rho \in P$, $e_\rho\sigma''\epsilon = \pm e_\rho$. We show in fact that $e_\rho\sigma''\epsilon = e_\rho$ always holds.

Let $\rho \in P$. Then $\rho = \rho_i + \sum_{k=1}^{l} n_k\hat\alpha_k$ for some nonnegative integers n_k. So $e_\rho \in \mathfrak{J}_i$ and for some $\varphi \in \Phi$, $e_\rho = \varphi[[CE''_{\rho_i}]\,D]$, where C and D are (possibly vacuous) Lie monomials in $E_{\hat\alpha_1}\,,..., E_{\hat\alpha_l}$. Suppose $e_\rho\sigma'\epsilon = e_\rho$. Then $E''_{\rho_i} = E'_{\rho_i}$, so that σ' and σ'' agree on $E_{\hat\alpha_1}\,,..., E_{\hat\alpha_l}\,, E''_{\rho_i}$. Consequently, $e_\rho\sigma' = e_\rho\sigma''$, i.e.,

$e_\rho \sigma'' \epsilon = e_\rho$. Suppose, on the other hand, that $e_\rho \sigma' \epsilon = -e_\rho$. Then $E''_{\rho_i} = \sqrt{-1}\, E'_{\rho_i}$, $F''_{\rho_i} = -\sqrt{-1}\, F'_{\rho_i}$ and

$$\begin{aligned} e_\rho \sigma'' \epsilon &= \varphi[[CE''_{\rho_i}]\, D]\, \sigma'' \epsilon = \varphi[[C\sigma', F''_{\rho_i}], D\sigma']\, \epsilon \\ &= -\varphi \sqrt{-1}\, [[C\sigma', F'_{\rho_i}], D\sigma']\, \epsilon \\ &= -\varphi \sqrt{-1}\, [[C, E'_{\rho_i}], D]\, \sigma' \epsilon \\ &= -\varphi[[C, E''_{\rho_i}], D]\, \sigma' \epsilon \\ &= -e_\rho \sigma' \epsilon = -(-e_\rho) = e_\rho . \end{aligned}$$

Thus in all cases $e_\rho \sigma'' \epsilon = e_\rho$, i.e., $e_\rho \sigma'' = e_\rho \epsilon = \bar{e}_\rho$. This completes the proof of the Lemma: σ'' is the desired automorphism.

Henceforth σ is as constructed in Lemma 2.

For $x, y \in \mathfrak{J}$ we use the notation $U_{x,y} = U_{x+y} - U_x - U_y$. The following formula will be useful: If $x, y, z \in \mathfrak{J}$ then

$$[x[y\bar{z}]] = zU_{x,y} .$$

This follows easily from the fact that $[y\bar{z}] = 2(R_{y\cdot z} - [R_y, R_z])$.

Since σ and ϵ both interchange $\mathfrak{J}$ and $\bar{\mathfrak{J}}$, $\sigma\epsilon$ stabilizes $\mathfrak{J}$. We note that in fact $\sigma\epsilon \mid \mathfrak{J}$ is an automorphism of $\mathfrak{J}$. Indeed, if $\rho \in P$, then $e_\rho \sigma \epsilon = \bar{e}_\rho \epsilon = e_\rho$ so that $\sigma\epsilon$ fixes $1 = \sum_{\rho \in P} e_\rho$. If we take $z = 1$ in the above formula, we get

$$\begin{aligned} (2x \cdot y)\, \sigma\epsilon &= (1U_{x,y})\, \sigma\epsilon = [x[y\bar{1}]]\, \sigma\epsilon \\ &= [x\sigma\epsilon, [y\sigma\epsilon, \bar{1}]] \\ &= 2x\sigma\epsilon \cdot y\sigma\epsilon, \end{aligned}$$

since $\bar{1}\sigma\epsilon = 1\epsilon\sigma\epsilon = 1\sigma\epsilon\epsilon = 1\epsilon$.

We now use the automorphism σ to construct a Chevalley basis for $\mathfrak{K}$. This is done as follows: For each root ρ of $\mathfrak{K}$ we choose $0 \neq K_\rho \in \mathfrak{K}_\rho$ so that the K_ρ's satisfy

$$K_\rho \sigma = K_{-\rho}, \qquad [K_\rho, K_{-\rho}] = H_\rho .$$

Such a choice is possible and is unique in the following sense: If $x \in \mathfrak{K}_\rho$ has the property that $[x, [x, x\sigma]] = 2x$, then $x = \pm K_\rho$ or 0. Indeed, $x = \lambda K_\rho$ for some $\lambda \in \Phi$, so that

$$2x = [x, [x, x\sigma]] = \lambda^3 [K_\rho, [K_\rho, K_\rho \sigma]] = \lambda^3 \cdot 2K_\rho = 2\lambda^2 x;$$

this clearly implies $x = 0$ or $\lambda^2 = 1$. The Chevalley Basis Theorem now says that the above-chosen K_ρ's (for all roots ρ of $\mathfrak{R}$) together with $H_{\rho_1}, \ldots, H_{\rho_r}$ form a Chevalley basis of $\mathfrak{R}$. The reader is referred to [1, Théorème 1] for the original proof of the Chevalley Basis Theorem; for a proof of the theorem in the form used here, see [4, p. 147] and [8, pp. 1–7]. Since the structure constants with respect to a Chevalley basis are integers, the Lie product of any two of our basis elements is an integral linear combination of the basis elements. Let $\mathfrak{R}_{\mathbf{Z}}$ be the (additive) abelian group generated by this basis. Let $\mathfrak{J}_{\mathbf{Z}}$ be the (additive) abelian group generated by those K_ρ for which $\mathfrak{R}_\rho \subseteq \mathfrak{J}$ (these form a basis of $\mathfrak{J}$, so that $\mathfrak{J}_{\mathbf{Z}} = \mathfrak{J} \cap \mathfrak{R}_{\mathbf{Z}}$). $\mathfrak{R}_{\mathbf{Z}}$ is closed under the Lie product.

We first show two things: $e_\rho = \pm K_\rho$ for all $\rho \in P$, and $K_\rho \epsilon = \pm K_{\rho\epsilon^*}$ for all roots ρ of $\mathfrak{R}$. By the above remarks, the following suffices:

$$\begin{aligned}
[e_\rho, [e_\rho, e_\rho\sigma]] &= [e_\rho, [e_\rho, \bar{e}_\rho]] = [e_\rho, H_\rho] \\
&= 2e_\rho, \\
[K_\rho\epsilon, [K_\rho\epsilon, K_\rho\epsilon\sigma]] &= [K_\rho\epsilon, [K_\rho\epsilon, K_\rho\sigma\epsilon]] \\
&= [K_\rho, [K_\rho, K_\rho\sigma]]\,\epsilon \\
&= 2K_\rho\epsilon.
\end{aligned}$$

In particular, $1 = \sum_{\rho\in P} e_\rho \in \mathfrak{J}_{\mathbf{Z}}$. Also $K \in \mathfrak{R}_{\mathbf{Z}}$ implies $K\epsilon \in \mathfrak{R}_{\mathbf{Z}}$.

(A further refinement in the choice of the K_ρ is possible: If $\mathfrak{R}_\rho \not\subseteq R_{\mathfrak{J}}$, one may arrange that $K_\rho\epsilon = K_{\rho\epsilon^*}$. If $\rho\epsilon^* = \rho$, then [2, p. 20] implies that either $K_\rho \in \mathfrak{D}$, in which case $K_\rho\epsilon = K_\rho$, or $K_\rho \in R_{\mathfrak{J}}$, which is the exceptional case. If $\rho\epsilon^* = -\rho$, then $\rho \neq \hat{\alpha}$ for any root α of $\mathfrak{L}'$; this is because ϵ^* stabilizes the positive roots of $\mathfrak{L}'$, and ρ, $-\rho$ cannot have the same sign. So $\mathfrak{R}_\rho$ is contained either in $\mathfrak{J}$ or $\bar{\mathfrak{J}}$, i.e., either $\rho \in P$ or $-\rho \in P$. Hence $\{K_\rho, K_{-\rho}\} = \{\pm e_\rho, \pm \bar{e}_\rho\}$. Since $e_\rho\sigma = \bar{e}_\rho$, $-e_\rho\sigma = -\bar{e}_\rho$, we must have $\{K_\rho, K_{-\rho}\} = \{e_\rho, \bar{e}_\rho\}$ or $\{-e_\rho, -\bar{e}_\rho\}$; in either case $K_\rho\epsilon = K_{-\rho} = K_{\rho\epsilon^*}$. Finally, if $\rho\epsilon^* \neq \pm\rho$ then ρ, $-\rho$, $\rho\epsilon^*$, $-\rho\epsilon^*$ are distinct roots. If $K_\rho\epsilon = \lambda K_{\rho\epsilon^*}$, $\lambda = \pm 1$, then $K_{-\rho}\epsilon = K_\rho\sigma\epsilon = K_\rho\epsilon\sigma = \lambda K_{-\rho\epsilon^*}$, $K_{\rho\epsilon^*}\epsilon = \lambda^{-1} K_\rho\epsilon\epsilon = \lambda K_\rho$, and similarly $K_{-\rho\epsilon^*}\epsilon = \lambda K_{-\rho}$; i.e., all four roots satisfy $K_\tau\epsilon = \lambda K_{\tau\epsilon^*}$. If $\lambda = +1$ there is nothing to prove. If $\lambda = -1$ then we replace $K_{\rho\epsilon^*}$ by $-K_{\rho\epsilon^*}$, $K_{-\rho\epsilon^*}$ by $-K_{-\rho\epsilon^*}$ in the Chevalley basis. The new basis is also a Chevalley basis, in which $K_\tau\epsilon = K_{\tau\epsilon^*}$ for $\tau = \pm\rho, \pm\rho\epsilon^*$.)

THEOREM 1. *If $x, y \in \mathfrak{J}_{\mathbf{Z}}$ then $yU_x \in \mathfrak{J}_{\mathbf{Z}}$.*

Proof. First note that if $x, y, z \in \mathfrak{J}_{\mathbf{Z}}$ then $zU_{x,y} = [x[y\bar{z}]] \in \mathfrak{R}_{\mathbf{Z}} \cap \mathfrak{J} = \mathfrak{J}_{\mathbf{Z}}$, since $\bar{z} = z\epsilon \in \mathfrak{R}_{\mathbf{Z}}$ and $\mathfrak{R}_{\mathbf{Z}}$ is closed under Lie product. Our object now is to show that if $\mathfrak{R}_\rho \subseteq \mathfrak{J}$ then U_{K_ρ} stabilizes $\mathfrak{J}_{\mathbf{Z}}$. Suppose this is shown. Then for $x = \sum_\rho n_\rho K_\rho \in \mathfrak{J}_{\mathbf{Z}}$ (where n_ρ are integers),

$$U_x = \sum_\rho n_\rho{}^2 U_{K_\rho} + \sum_{\rho,\tau} n_\rho n_\tau U_{K_\rho, K_\tau},$$

where the second summation is taken over unordered pairs ρ, τ. Since U_{K_ρ}, U_{K_ρ, K_τ} stabilize $\mathfrak{J}_{\mathbf{Z}}$, U_x also stabilizes $\mathfrak{J}_{\mathbf{Z}}$ and the theorem is proven.

(1) Let $x \in \mathfrak{R}_\rho \subseteq \mathfrak{J}_{\mathbf{Z}}$, where ρ is a root of $\mathfrak{R}$. Then $U_x U_{x\sigma\epsilon}$ stabilizes each root space $\mathfrak{R}_\tau$ such that $\mathfrak{R}_\tau \subseteq \mathfrak{J}$. For if $y \in \mathfrak{R}_\tau$, then

$$\begin{aligned} 4yU_xU_{x\sigma\epsilon} &= 2yU_xU_{x\sigma\epsilon, x\sigma\epsilon} \\ &= 2[x\sigma\epsilon, [x\sigma\epsilon, \overline{yU_x}]] \\ &= [x\sigma\epsilon, [x\sigma\epsilon, [x[x\bar{y}]]\,\epsilon]] \\ &= [x\sigma\epsilon, [x\sigma\epsilon, [\bar{x}[\bar{x}y]]]]. \end{aligned}$$

Since $\bar{x} \in \mathfrak{R}_{\rho\epsilon^*}$ and $x\sigma\epsilon \in \mathfrak{R}_{-\rho\epsilon^*}$, we see that $yU_xU_{x\sigma\epsilon}$ belongs to the root space of $-\rho\epsilon^* - \rho\epsilon^* + \rho\epsilon^* + \rho\epsilon^* + \tau = \tau$.

(2) Let $x = K_\rho$, $y = K_\tau$, where $\mathfrak{R}_\rho$, $\mathfrak{R}_\tau \subseteq \mathfrak{J}$. Then $yU_xU_{x\sigma\epsilon}$ equals 0 or y. For (1) implies that $yU_xU_{x\sigma\epsilon} = \lambda y$, where λ is some element of Φ. Also $2x = [x, [x, x\sigma]] = [x, [x, \overline{x\sigma\epsilon}]] = 2(x\sigma\epsilon)\, U_x$. Hence

$$\begin{aligned} \lambda^2 y = y(U_xU_{x\sigma\epsilon})^2 &= yU_xU_{x\sigma\epsilon}U_xU_{x\sigma\epsilon} \\ &= yU_{x\sigma\epsilon U_x}U_{x\sigma\epsilon} = yU_xU_{x\sigma\epsilon} = \lambda y. \end{aligned}$$

Thus $y = 0$ (in which case the result is clear) or $\lambda^2 = \lambda$ (in which case $\lambda = 0$ or 1).

(3) Let $x = K_\rho$, $y = K_\tau$, where $\mathfrak{R}_\rho$, $\mathfrak{R}_\tau \subseteq \mathfrak{J}$. Then yU_x is either zero or $\pm K_{2\rho+\tau\epsilon^*}$. Certainly, $2yU_x = [x[x\bar{y}]]$ belongs to the root space of $2\rho + \tau\epsilon^*$, which is zero if $2\rho + \tau\epsilon^*$ is not a root. So if $0 \neq z = yU_x$, we need only show that $[z, [z, z\sigma]] = 2z$. Since

$$[z, [z, z\sigma]] = [z, [z, \overline{z\sigma\epsilon}]] = 2(z\sigma\epsilon)\, U_z,$$

it is sufficient to show that $(z\sigma\epsilon)U_z = z$. The hypotheses $x = K_\rho$, $y = K_\tau$ imply that $(x\sigma\epsilon)U_x = x$, $(y\sigma\epsilon)U_y = y$.

Now $z \neq 0$ implies that $yU_xU_{x\sigma\epsilon} = y$; otherwise (2) yields $0 = yU_xU_{x\sigma\epsilon}$, and if we act on both sides of this equation with U_x we obtain

$$0 = yU_xU_{x\sigma\epsilon}U_x = yU_{(x\sigma\epsilon)U_x} = yU_x = z.$$

Finally,

$$\begin{aligned}(z\sigma\epsilon)\, U_z &= (yU_x)\, \sigma\epsilon U_{yU_x} = (yU_x)\, \sigma\epsilon U_x U_y U_x \\ &= (yU_x U_{x\sigma\epsilon})\, \sigma\epsilon U_y U_x = (y\sigma\epsilon)\, U_y U_x \\ &= yU_x = z,\end{aligned}$$

which proves (3).

Since $\mathfrak{J}_{\mathbf{Z}}$ is generated by those K_τ belonging to $\mathfrak{J}$ and U_x is linear, (3) implies that $\mathfrak{J}_{\mathbf{Z}} U_x \subseteq \mathfrak{J}_{\mathbf{Z}}$. This completes the proof of the theorem.

Theorem 1 implies that $\mathfrak{J}_{\mathbf{Z}}$ is an *order* of $\mathfrak{J}$, in the sense of Knebusch [6, p. 175] (strictly speaking, $\mathfrak{J}_{\mathbf{Z}}$ is an order of $\mathfrak{J}_{\mathbf{Q}} = \mathfrak{J}_{\mathbf{Z}} \otimes {}_{\mathbf{Z}}\mathbf{Q}$, where $\mathbf{Q}$ denotes the rational numbers).

3. The Generic Trace

Let t be the generic trace of $\mathfrak{J}$. Our purpose in this section is to find the matrix of the generic trace bilinear form $t(x, y) \equiv t(x \cdot y)$ with respect to the basis of $\mathfrak{J}$ chosen in Section 2. In particular, it will be shown that this matrix is a monomial matrix with entries 0, ± 1, ± 2.

Lemma 3. *Let $\rho \in P$ and suppose τ is a root such that $\mathfrak{R}_\tau \subseteq \mathfrak{J}_{\rho\rho}$, but $\tau \neq \rho$. Let $0 \neq x \in \mathfrak{R}_\tau$. Then*

(a) *$0 \neq R_x \in \mathfrak{R}_{\tau-\rho}$ and $[R_x, R_{e_\rho}] = 0$;*

(b) *$\rho - 2\tau$ and $\rho + \tau$ are not roots, and $x^{\cdot 2} = 0$.*

Proof. (a) Since $\bar{e}_\rho \in \mathfrak{R}_{-\rho}$, we see that $[x, \bar{e}_\rho] \in \mathfrak{R}_{\tau-\rho}$. Now $[x, \bar{e}_\rho] = 2(R_{x \cdot e_\rho} - [R_x, R_{e_\rho}]) = 2(R_x - [R_x, R_{e_\rho}])$. But $[R_x, R_{e_\rho}] = 0$ (this follows from [5, p. 34]: in identity (O_1) take $b = x$, $c = d = e_\rho$). So $[x, \bar{e}_\rho] = 2R_x$.

(b) $(\rho + \tau)(R_1) = 2$, so $\rho + \tau$ is not a root [2, Proposition 6]. Since $[x, R_x] = x^{\cdot 2}$, we see that $2\tau - \rho$ is a root if and only if $x^{\cdot 2} \neq 0$. Suppose $x^{\cdot 2} \neq 0$. Then $x^{\cdot 2} \in \mathfrak{J}_{\rho\rho}$ (which is a subalgebra of $\mathfrak{J}$). Also $2\tau - \rho \neq \rho$, since otherwise $\rho = \tau$. So the hypotheses on τ also apply to $2\tau - \rho$ and (a) says that $[x^{\cdot 2}, \bar{e}_\rho] = 2R_{x^{\cdot 2}}$ is a root vector for $2\tau - \rho - \rho = 2(\tau - \rho)$. This is a contradiction: $\tau - \rho$ and $2(\tau - \rho)$ cannot both be roots of $\mathfrak{R}$. So $2\tau - \rho$ is not a root, and hence neither is $\rho - 2\tau$.

Lemma 4. *Let $\rho \in P$ and suppose τ, ν are roots of $\mathfrak{R}$ such that $\mathfrak{R}_\nu \subseteq \mathfrak{J}_{\rho\rho}$, $\mathfrak{R}_\tau \subseteq \mathfrak{J}_{\rho\rho}$, $\nu \neq \rho$, $\tau \neq \rho$. Let $x = K_\tau$, $y = K_\nu$.*

(a) *If $\nu = -\tau\epsilon^*$, then $x \cdot y = \pm\frac{1}{2}\, e_\rho$ and $\tau - \tau\epsilon^* = 2\rho$.*

(b) *If $\nu \neq -\tau\epsilon^*$, then $x \cdot y = 0$.*

Proof. First note that $\mathfrak{R}_{-\tau\epsilon^*} = \mathfrak{R}_\tau \sigma\epsilon \subseteq \mathfrak{J}_{\rho\rho}$ since $\sigma\epsilon$ stabilizes the Peirce spaces (it is an automorphism of $\mathfrak{J}$ which fixes the idempotents e_ρ). Also $-\tau\epsilon^* \neq \rho$ since $\rho = -\rho\epsilon^*$.

(a) If $\mu \in P$, $\mu \neq \rho$ then $x, y, x \cdot y \in \mathfrak{J}_0(e_\mu)$, hence $yU_{x,e_\mu} = 0$. Thus

$$2x \cdot y = yU_{x,1} = \sum_{\mu \in P} yU_{x,e_\mu} = yU_{x,e_\rho} = [e_\rho[x\bar{y}]].$$

Now $\bar{y} = K_{-\tau\epsilon^*\epsilon} = \pm K_{-\tau}$, so that

$$2x \cdot y = \pm [e_\rho, H_\tau] = \pm\rho(H_\tau)\, e_\rho = \pm \frac{2(\rho, \tau)}{(\tau, \tau)}\, e_\rho .$$

But $2(\rho, \tau)/(\tau, \tau) = 1$ since the τ-string of roots through ρ is $\rho - \tau$, ρ, by Lemma 3(b). So $2x \cdot y = \pm e_\rho$, as desired.

Since $x \cdot y = yR_x = [y, R_x]$ is a root vector for $-\tau\epsilon^* + \tau - \rho$, we find that $-\tau\epsilon^* + \tau - \rho = \rho$, i.e., $\tau - \tau\epsilon^* = 2\rho$.

(b) Assume $x \cdot y \neq 0$. Then $x \cdot y = [x, R_y]$ and $R_y \in \mathfrak{R}_{\nu-\rho}$, so that $\tau + \nu - \rho$ is a root and $x \cdot y \in \mathfrak{R}_{\tau+\nu-\rho}$. But $\tau + \nu - \rho \neq \rho$: otherwise $\tau + \nu = 2\rho = \tau - \tau\epsilon^*$ (by (a)) and $\nu = -\tau\epsilon^*$. Also $x \cdot y \in \mathfrak{J}_{\rho\rho}$. Lemma 3(a) implies that $R_{x\cdot y} \in \mathfrak{R}_{\tau+\nu-2\rho}$.

Now $[x, \bar{y}] = 2(R_{x\cdot y} - [R_x, R_y])$ is a root vector for

$$\tau + \nu\epsilon^* = \tau + \nu + \nu\epsilon^* - \nu = \tau + \nu - 2\rho$$

(applying (a) to ν), so that $2R_{x\cdot y} - 2[R_x, R_y]$ and $R_{x\cdot y}$ must be scalar multiples of each other. This implies that $[R_x, R_y] = 0$.

Let $z = K_{-\tau\epsilon^*}$. If $(y \cdot z) \cdot x = 0$, then

$$0 = (y \cdot z) \cdot x = y \cdot (z \cdot x) = y \cdot (\pm \tfrac{1}{2} e_\rho) = \pm \tfrac{1}{2} y,$$

by (a). This contradiction shows that $(y \cdot z) \cdot x \neq 0$. Now $y \cdot z = [z, R_y]$ belongs to the root space of $-\tau\epsilon^* + \nu - \rho$, which is not equal to $-\tau\epsilon^*$ (otherwise $\nu = \rho$). We claim that $[R_{y\cdot z}, R_x] = 0$. If $-\tau\epsilon^* + \nu - \rho = \rho$ this follows from Lemma 3(a): $R_{y\cdot z}$ is a multiple of R_{e_ρ}. If $-\tau\epsilon^* + \nu - \rho \neq \rho$ then our hypotheses on ν and τ also apply to $-\tau\epsilon^* + \nu - \rho$ and τ, and this follows in the same way as our proof that $[R_x, R_y] = 0$.

Finally, $((y \cdot z) \cdot x) \cdot x = (y \cdot z) \cdot (x \cdot x) = (y \cdot z) \cdot 0 = 0$ by Lemma 3(b) and $((y \cdot z) \cdot x) \cdot x = (y \cdot (z \cdot x)) \cdot x = (y \cdot (\pm \tfrac{1}{2} e_\rho)) \cdot x = \pm \tfrac{1}{2} y \cdot x \neq 0$ by (a). This contradiction completes the proof.

(We remark that if the basis elements K_ρ have been chosen so that $K_\rho\epsilon = K_{\rho\epsilon^*}$ whenever $K_\rho \notin R_{\mathfrak{J}}$, then one can strengthen Lemma 4(a) and conclude that $x \cdot y = + \tfrac{1}{2} e_\rho$, as is clearly seen by an inspection of the above proof.)

LEMMA 5. *Let ρ, τ, x be as in Lemma 3. Let $y = K_{-\tau\epsilon^*}$ and suppose (by Lemma 4) that $x \cdot y = (s/2)\, e_\rho$, where $s = \pm 1$. Then $\frac{1}{2}(e_\rho + x + sy)$ and $\frac{1}{2}(e_\rho - x - sy)$ are orthogonal primitive idempotents whose sum is e_ρ.*

Proof. The sum of these two elements is clearly e_ρ. Also

$$\begin{aligned}\tfrac{1}{4}(e_\rho \pm (x + sy))^{\cdot 2} &= \tfrac{1}{4}(e_\rho^{\cdot 2} + x^{\cdot 2} + s^2 y^{\cdot 2} \pm 2e_\rho \cdot x \pm 2se_\rho \cdot y + 2sx \cdot y)\\ &= \tfrac{1}{4}(e_\rho + 0 + 0 \pm 2x \pm 2sy + s^2 e_\rho)\\ &= \tfrac{1}{2}(e_\rho \pm x \pm sy),\end{aligned}$$

and

$$\begin{aligned}(e_\rho + x + sy) \cdot (e_\rho - x - sy) &= e_\rho^{\cdot 2} - (x + sy)^{\cdot 2}\\ &= e_\rho - x^{\cdot 2} - s^2 y^{\cdot 2} - 2sx \cdot y\\ &= e_\rho - 0 - 0 - s^2 e_\rho\\ &= e_\rho - e_\rho = 0.\end{aligned}$$

So these elements are orthogonal idempotents, and it remains only to show that they are primitive. Their 1-Peirce spaces are contained in $\mathfrak{J}_{\rho\rho}$. If $\sum_\nu z_\nu$ belongs to $\mathfrak{J}_1(\frac{1}{2}(e_\rho \pm (x + sy)))$, where the sum is extended over all roots ν such that $\mathfrak{R}_\nu \subseteq \mathfrak{J}_{\rho\rho}$ and where $z_\nu \in \mathfrak{R}_\nu$, then

$$\begin{aligned}\sum_\nu z_\nu &= \Big(\sum_\nu z_\nu\Big) \cdot \tfrac{1}{2}(e_\rho \pm (x + sy))\\ &= \tfrac{1}{2}\Big(\sum_\nu z_\nu \pm z_\rho \cdot x \pm z_{-\tau\epsilon^*} \cdot x \pm sz_\rho \cdot y \pm sz_\tau \cdot y\Big)\end{aligned}$$

by Lemma 4(b). Since $z_\rho \cdot x$ and $z_\rho \cdot y$ are scalar multiples of x and y, respectively, while $z_{-\tau\epsilon^*} \cdot x$ and $z_\tau \cdot y$ are scalar multiples of e_ρ, we can equate components.

$$\begin{aligned}&z_\nu = \tfrac{1}{2} z_\nu \quad \text{if} \quad \nu \neq \rho, \tau, -\tau\epsilon^*, &&\text{i.e.,} \quad z_\nu = 0,\\ &z_\tau = \tfrac{1}{2}(z_\tau \pm z_\rho \cdot x), &&\text{i.e.,} \quad z_\tau = \pm z_\rho \cdot x,\\ &z_{-\tau\epsilon^*} = \tfrac{1}{2}(z_{-\tau\epsilon^*} \pm sz_\rho \cdot y), &&\text{i.e.,} \quad z_{-\tau\epsilon^*} = \pm sz_\rho \cdot y.\end{aligned}$$

So $\sum_\nu z_\nu = z_\rho \pm z_\rho \cdot x \pm sz_\rho \cdot y = z_\rho \cdot (e_\rho \pm (x + sy))$, and this means (since z_ρ is a scalar multiple of e_ρ) that $\sum_\nu z_\nu$ is a scalar multiple of $\frac{1}{2}(e_\rho \pm (x + sy))$. This completes the proof: The 1-Peirce spaces of these idempotents are one-dimensional, and hence the idempotents are primitive.

We recall that if e is a primitive idempotent of $\mathfrak{J}$, then $t(e) = 1$. This well-known fact may be seen either by explicit computation of the generic trace of each of the simple algebras, using the classification theory [5, pp. 230–233], or by the following argument, which does not use the classification theory. Embed e in a complete set of orthogonal primitive idempotents. The space spanned by these idempotents is a Cartan subalgebra of $\mathfrak{J}$ and contains an associator regular element (see [5, especially Theorem 25 on p. 354 and the remarks on p. 352 preceding Theorem 23]). Then by the proof of Theorem 24 in [5, p. 353], the generic trace and the reduced trace on $\mathfrak{J}$ constructed from this set of idempotents are identical. In particular, $t(e) = 1$.

The last lemma has the following

COROLLARY. *If* $\rho \in P$ *is such that* $\dim \mathfrak{J}_{\rho\rho} = 1$, *then* $t(e_\rho) = 1$. *Otherwise* $t(e_\rho) = 2$.

Proof. If $\dim \mathfrak{J}_{\rho\rho} = 1$ then e_ρ is primitive. Otherwise e_ρ is the sum of two primitive idempotents.

LEMMA 6. *Suppose* $\rho, \rho' \in P$ *and* $\rho \neq \rho'$. *Suppose* $0 \neq x \in \mathfrak{R}_\tau \subseteq \mathfrak{J}_{\rho\rho'}$.

(a) *If* $x^{\cdot 2} = 0$ *then neither* $2\tau - \rho$ *nor* $2\tau - \rho'$ *are roots;*

(b) *If* $x^{\cdot 2} \neq 0$ *then either* $x^{\cdot 2} \in \mathfrak{R}_{2\tau-\rho} \subseteq \mathfrak{J}_{\rho'\rho'}$ *and* $2\tau - \rho'$ *is not a root, or* $x^{\cdot 2} \in \mathfrak{R}_{2\tau-\rho'} \subseteq \mathfrak{J}_{\rho\rho}$ *and* $2\tau - \rho$ *is not a root.*

Proof. $x^{\cdot 2} = y + z$ where $y \in \mathfrak{J}_{\rho\rho}$ and $z \in \mathfrak{J}_{\rho'\rho'}$. Now

$$[x, \bar{e}_\rho] = 2(R_{x\cdot e_\rho} - [R_x, R_{e_\rho}]) = R_x - 2[R_x, R_{e_\rho}]$$

is not zero (since $x \neq 0$) and so is a root vector for $\tau - \rho$. Also

$$\begin{aligned}[x, R_x - 2[R_x, R_{e_\rho}]] &= x^{\cdot 2} - 2x^{\cdot 2} \cdot e_\rho + 2x \cdot (x \cdot e_\rho) \\ &= x^{\cdot 2} - 2y + x^{\cdot 2} \\ &= 2(x^{\cdot 2} - y) = 2z.\end{aligned}$$

So z is nonzero if and only if $\tau + (\tau - \rho) = 2\tau - \rho$ is a root, in which case $z \in \mathfrak{R}_{2\tau-\rho}$. Similarly, y is nonzero if and only if $2\tau - \rho'$ is a root, in which case $y \in \mathfrak{R}_{2\tau-\rho'}$. If $x^{\cdot 2} = 0$, then $y = z = 0$ and (a) is clear. To show (b) we need only show that it is not possible for both y and z to be nonzero. Suppose that $z \neq 0 \neq y$. Then by Lemma 3(a), $R_y \in \mathfrak{R}_{2\tau-\rho'-\rho}$ and $R_z \in \mathfrak{R}_{2\tau-\rho-\rho'}$. This means either that $2\tau - \rho - \rho' = 0$ or that R_y, R_z are scalar multiples of each other. The latter is impossible since in that case y and z would be proportional and we would have $2\tau - \rho = 2\tau - \rho'$, contrary to $\rho \neq \rho'$. The former is also impossible, for if $2\tau - \rho - \rho' = 0$ then the fact that $\rho(\mathfrak{W}) = \rho'(\mathfrak{W}) = 0$ would imply that $\tau(\mathfrak{W}) = 0$, i.e., that $\tau \in P$. This is a contradiction to the assumption that $\mathfrak{R}_\tau \subseteq \mathfrak{J}_{\rho\rho'}$. The proof is thus complete.

In the proof of the next lemma we will want to use the following well-known fact: If $\mathfrak{A}$ is a simple, finite-dimensional algebra over an algebraically closed field and if $t_1(\,,\,)$ and $t_2(\,,\,)$ are two associative symmetric bilinear forms on $\mathfrak{A}$, then t_1 and t_2 are proportional. For completeness we offer the following proof of this. First, since the radical of an associative symmetric bilinear form is an ideal, such a form on $\mathfrak{A}$ is either zero or is nondegenerate. Consequently we can assume that t_1, t_2 are nondegenerate. Let A be the unique linear transformation of $\mathfrak{A}$ such that $t_1(xA, y) = t_2(x, y)$ for all $x, y \in \mathfrak{A}$. Let x be an eigenvector of A and α the corresponding eigenvalue. Then for all $y \in \mathfrak{A}$, $t_2(x, y) - \alpha t_1(x, y) = t_2(x, y) - t_1(xA, y) = 0$. That is, x is in the radical of the associative symmetric bilinear form $t_2 - \alpha t_1$. So $t_2 - \alpha t_1 = 0$, i.e., $t_2 = \alpha t_1$.

Returning to the algebra $\mathfrak{R}$, we observe that $\mathfrak{D}$ and $R_{\mathfrak{J}}$ are orthogonal with respect to the Killing form $(\,,\,)$ of $\mathfrak{R}$ and that this implies that the form $t_1(x, y) = (R_x, R_y)$ on $\mathfrak{J}$ is associative. Indeed, if $D \in \mathfrak{D}$ and $x, y \in \mathfrak{J}$, then

$$\bar{y} \operatorname{ad} D \operatorname{ad} R_x = -\overline{y \operatorname{ad} D \operatorname{ad} R_x}\,.$$

Also $\operatorname{ad} D \operatorname{ad} R_x$ sends $\mathfrak{D} \to R_{\mathfrak{J}}$ and $R_{\mathfrak{J}} \to \mathfrak{D}$. These two facts clearly imply that $(D, R_x) = \operatorname{Tr} \operatorname{ad} D \operatorname{ad} R_x = 0$. And if $x, y, z \in \mathfrak{J}$ then

$$\begin{aligned}(R_{x\cdot y}, R_z) &= (R_{x\cdot y}, R_z) - ([R_x, R_y], R_z)\\ &= \tfrac{1}{2}([x, \bar{y}], R_z) = -\tfrac{1}{2}([\bar{y}, x], R_z)\\ &= -\tfrac{1}{2}(\bar{y}, [x, R_z]) = -\tfrac{1}{2}(\bar{y}, x \cdot z).\end{aligned}$$

The last expression is symmetric in x and z. So $(R_{x\cdot y}, R_z) = (R_x, R_{y\cdot z})$.

LEMMA 7. *Suppose ρ, ρ', x, τ are as in Lemma 6.*

(a) *If $x^{\cdot 2} = 0$ then $t(e_\rho) = t(e_{\rho'})$.*

(b) *If $0 \neq x^{\cdot 2} \in \mathfrak{J}_{\rho\rho}$ then $t(e_\rho) = 2$ and $t(e_{\rho'}) = 1$.*

Proof. We first show that in either case $t(e_\rho)(\rho, \rho) = t(e_{\rho'})(\rho', \rho')$. Since $\mathfrak{J}_{\rho\rho'} \neq 0$, e_ρ and $e_{\rho'}$ are connected idempotents and must belong to the same simple summand $\mathfrak{J}_i$ of $\mathfrak{J}$. The generic trace form $t(\,,\,)$ and the form $t_1(\,,\,)$ defined above are two associative symmetric bilinear forms on $\mathfrak{J}$, so their restrictions to $\mathfrak{J}_i$ are proportional. Choose $\alpha \in \Phi$ such that $t(x \cdot y) = \alpha(R_x, R_y)$ for all $x, y \in \mathfrak{J}_i$. Then if H_ρ' is that element of $\mathfrak{H}$ such that $(H_\rho', H) = \rho(H)$ for all $H \in \mathfrak{H}$, we have

$$\begin{aligned}t(e_\rho) &= t(e_\rho \cdot e_\rho) = \alpha(R_{e_\rho}, R_{e_\rho})\\ &= \frac{\alpha}{4}(H_\rho, H_\rho) = \frac{\alpha}{4}\frac{4}{(\rho, \rho)^2}(H_\rho', H_\rho') \qquad [4, \text{p. } 112]\\ &= \frac{\alpha}{(\rho, \rho)^2}(\rho, \rho) = \frac{\alpha}{(\rho, \rho)}\,.\end{aligned}$$

We conclude that $t(e_\rho)(\rho, \rho) = \alpha$. Similarly, $t(e_{\rho'})(\rho', \rho') = \alpha$.

We know that τ, $\tau - \rho$ are roots (the latter with root vector $R_x - 2[R_x, R_{e_\rho}]$, as in the proof of Lemma 6); $\tau - 2\rho$ is not a root since

$$[\bar{e}_\rho, R_x - 2[R_x, R_{e_\rho}]] = -\overline{e_\rho \cdot x} - 2\overline{((x \cdot e_\rho) \cdot e_\rho - x \cdot e_\rho^{\cdot 2})}$$
$$= -\tfrac{1}{2}\bar{x} - 2(\tfrac{1}{4}\bar{x} - \tfrac{1}{2}\bar{x}) = 0.$$

And $(\tau + \rho)(R_1) = 2$ so that $\tau + \rho$ is not a root. We conclude that $2(\rho, \tau)/(\rho, \rho) = 1$. Similarly, $2(\rho', \tau)/(\rho', \rho') = 1$.

(a) If $x^{\cdot 2} = 0$ then neither $2\tau - \rho$ nor $2\tau - \rho'$ are roots, by Lemma 6. That is, the τ-string of roots through ρ (respectively ρ') is ρ, $\rho - \tau$ (respectively ρ', $\rho' - \tau$). Hence $2(\rho, \tau)/(\tau, \tau) = 1 = 2(\rho', \tau)/(\tau, \tau)$. This together with the above implies that $(\rho', \rho') = 2(\rho', \tau) = 2(\rho, \tau) = (\rho, \rho)$ and therefore that $t(e_\rho) = t(e_{\rho'})$.

(b) If $0 \neq x^{\cdot 2} \in \mathfrak{J}_{\rho\rho}$, then $2\tau - \rho'$ is a root and $2\tau - \rho$ is not. So the τ string of roots through ρ (respectively ρ') is ρ, $\rho - \tau$ (respectively ρ', $\rho' - \tau$, $\rho' - 2\tau$) and $2(\rho, \tau)/(\tau, \tau) = 1$, while $2(\rho', \tau)/(\tau, \tau) = 2$. As before, this means that $2(\rho, \tau) = (\tau, \tau) = (\rho', \tau)$ and $(\rho', \rho') = 2(\rho', \tau) = 4(\rho, \tau) = 2(\rho, \rho)$, and hence that $t(e_\rho) = t(e_{\rho'})(\rho', \rho')/(\rho, \rho) = 2t(e_{\rho'})$. By the Corollary to Lemma 5, $t(e_\rho) = 2$. So $t(e_{\rho'}) = 1$.

THEOREM 2. *Suppose μ, ν are roots of $\mathfrak{R}$ such that $\mathfrak{R}_\mu$, $\mathfrak{R}_\nu \subseteq \mathfrak{J}$. Let $x = K_\mu$, $y = K_\nu$. Then $t(x, y) = 0$ unless $\nu = -\mu\epsilon^*$. If $\nu = -\mu\epsilon^*$, then one of the following occurs*:

(a) *$\mu \in P$ and $t(x, y) = t(e_\mu) = 1$ or 2.*

(b) *$\mu \notin P$ and $x, y \in \mathfrak{J}_{\rho\rho}$ for some $\rho \in P$; in this case $t(x, y) = \pm 1$.*

(c) *$x, y \in \mathfrak{J}_{\rho\rho'}$ for some ρ, $\rho' \in P$ $(\rho \neq \rho')$ and $x^{\cdot 2} = 0$; in this case $t(x, y) = \pm t(e_\rho) = \pm 1$ or ± 2.*

(d) *$x, y \in \mathfrak{J}_{\rho\rho'}$ for some $\rho, \rho' \in P$ $(\rho \neq \rho')$ and $x^{\cdot 2} \neq 0$; in this case $t(x, y) = \pm 2$.*

Proof. The form t_2 on $\mathfrak{J}$ defined by $t_2(a, b) = (a, \bar{b})$ is symmetric and associative: $(a, \bar{b}) = (a\epsilon, \bar{b}\epsilon) = (\bar{a}, b)$ and

$$(a \cdot c, \bar{b}) = ([a, R_c], \bar{b}) = (a, [R_c, \bar{b}])$$
$$= -(a, [\bar{b}, R_c]) = (a, \overline{b \cdot c}).$$

Suppose x, y belong to different simple summands of $\mathfrak{J}$. Then $t(x, y) = t(x \cdot y) = t(0) = 0$. If x, y belong to the same simple summand $\mathfrak{J}_i$, choose $\alpha \in \Phi$ such that $t(a, b) = \alpha t_2(a, b)$ for all $a, b \in \mathfrak{J}_i$. Then $t(x, y) = \alpha t_2(x, y) = \alpha(x, \bar{y}) = \alpha(K_\mu, K_\nu\epsilon) = \pm\alpha(K_\mu, K_{\nu\epsilon^*})$. Now by [4,

p. 108, I], $(K_\mu, K_{\nu\epsilon^*}) = 0$ unless $\mu = -\nu\epsilon^*$. This proves the first part of the theorem.

Suppose $\nu = -\mu\epsilon^*$. Since $\sigma\epsilon$ fixes each $e_\rho (\rho \in P)$, $\sigma\epsilon$ stabilizes all the Peirce spaces $\mathfrak{J}_{\rho\rho'}$. But $x\sigma\epsilon = K_{-\mu}\epsilon = \pm K_{-\mu\epsilon^*} = \pm y$, so that x, y must belong to the same Peirce space $\mathfrak{J}_{\rho\rho'}$.

If $\rho = \rho'$ and $\mu = \rho$ then $-\rho\epsilon^* = \rho$ so that $\nu = \rho$ also. This means $x = y = K_\rho = \pm e_\rho$. Consequently, $t(x \cdot y) = t(e_\rho) = 1$ or 2, by the corollary to Lemma 5. This proves (a).

In general, $t(x, y) = t(x \cdot y) = \frac{1}{2} t([1, [x, \bar{y}]])$. But

$$[x, \bar{y}] = [K_\mu, K_{-\mu\epsilon^*}\epsilon] = [K_\mu, \pm K_{-\mu}] = \pm H_\mu .$$

So

$$\begin{aligned} t(x, y) &= \pm \tfrac{1}{2} t([1, H_\mu]) \\ &= \pm \tfrac{1}{2} \sum_{\rho \in P} t([e_\rho, H_\mu]) \\ &= \pm \tfrac{1}{2} \sum_{\rho \in P} \rho(H_\mu)\, t(e_\rho) = \pm \tfrac{1}{2} \sum_{\rho \in P} \frac{2(\rho, \mu)}{(\mu, \mu)} t(e_\rho). \end{aligned}$$

We compute $2(\rho, \mu)/(\mu, \mu)$ using the usual facts about root strings. We saw in Section 2 that $\mu - \rho$ is a root if and only if $\mathfrak{R}_\mu \subseteq \mathfrak{J}_1(e_\rho) \oplus \mathfrak{J}_{1/2}(e_\rho)$. Of course $\mu + \rho$ is never a root (since $(\mu + \rho)(R_1) = 2$). Thus if $x \in \mathfrak{J}_{\rho\rho'}$ and $\rho \neq \rho'' \neq \rho'$ then $2(\rho'', \mu)/(\mu, \mu) = 0$. That is,

$$t(x, y) = \begin{cases} \pm \dfrac{1}{2} \cdot \dfrac{2(\rho, \mu)}{(\mu, \mu)} t(e_\rho) & \text{if} \quad \rho = \rho', \\ \pm \dfrac{1}{2} \left[\dfrac{2(\rho, \mu)}{(\mu, \mu)} t(e_\rho) + \dfrac{2(\rho', \mu)}{(\mu, \mu)} t(e_{\rho'}) \right] & \text{if} \quad \rho \neq \rho'. \end{cases}$$

(b) In this case $\mu \neq \rho$ and $\rho = \rho'$. Then Lemma 3 shows that $\rho - 2\mu$, $\rho + \mu$ are not roots, but $\rho - \mu$ is. So $2(\rho, \mu)/(\mu, \mu) = 1$. The corollary to Lemma 5 shows that $t(e_\rho) = 2$. Hence $t(x, y) = \pm \frac{1}{2} \cdot 1 \cdot 2 = \pm 1$.

(c) In this case $\rho \neq \rho'$ and $x^{\cdot 2} = 0$. Then Lemma 6(a) shows that $\rho - 2\mu$, $\rho' - 2\mu$ are not roots, while of course $\rho - \mu$, $\rho' - \mu$ are. So $2(\rho, \mu)/(\mu, \mu) = 2(\rho', \mu)/(\mu, \mu) = 1$. Lemma 7(a) shows that $t(e_\rho) = t(e_{\rho'})$. So $t(x, y) = \pm \frac{1}{2} [t(e_\rho) + t(e_{\rho'})] = \pm t(e_\rho)$.

(d) In this case $\rho \neq \rho'$ and $0 \neq x^{\cdot 2} \in \mathfrak{J}_{\rho\rho}$ or $\mathfrak{J}_{\rho'\rho'}$ by Lemma 6(b). We choose notation so that $x^{\cdot 2} \in \mathfrak{J}_{\rho\rho}$. Then by Lemma 6(b), $\rho' - 2\mu$ is a root while $\rho - 2\mu$ is not. Of course, $\rho' - \mu$ is a root and $\rho' - 3\mu$ is not (since $(\rho' - 3\mu)(R_1) = -2$). Hence $2(\rho, \mu)/(\mu, \mu) = 1$ and $2(\rho', \mu)/(\mu, \mu) = 2$. Also Lemma 7(b) shows that $t(e_\rho) = 2$ and $t(e_{\rho'}) = 1$. Hence $t(x, y) = \pm \frac{1}{2} [1 \cdot 2 + 2 \cdot 1] = \pm 2$.

COROLLARY 1. *The matrix of the generic trace bilinear form on $\mathfrak{J}$ with respect to the basis $\{K_\rho \mid \mathfrak{R}_\rho \subseteq \mathfrak{J}\}$ of $\mathfrak{J}$ has exactly one nonzero entry in each row and in each column. These nonzero entries are ± 1, ± 2.*

(We observe that if the basis of $\mathfrak{R}$ has been chosen so that $K_\rho\epsilon = K_{\rho\epsilon^*}$ whenever $K_\rho \notin R_{\mathfrak{J}}$, then all the $\pm$ signs in the statement and proof of Theorem 2 and Corollary 1 may be replaced by $+$ signs.)

K.-H. Helwig has pointed out to the author that the following well-known fact is a consequence of the above.

COROLLARY 2. *Every finite-dimensional complex semisimple Jordan algebra has a compact real form.*

Proof. In the above we take $\Phi = \mathbf{C}$, the complex numbers. We choose the Chevalley basis of $\mathfrak{R}$ so that $K_\rho\epsilon = K_{\rho\epsilon^*}$ whenever $K_\rho \notin R_{\mathfrak{J}}$. Then the desired compact real form of $\mathfrak{J}$ is $\mathfrak{A} = \{\sum_\rho \lambda_\rho K_\rho \mid \lambda_{-\rho\epsilon^*} = \bar{\lambda}_\rho\}$, where the sum is extended over roots ρ such that $\mathfrak{R}_\rho \subseteq \mathfrak{J}$. $\mathfrak{A}$ is clearly a vector space over the real numbers $\mathbf{R}$ with basis $\{K_\rho + K_{-\rho\epsilon^*}, iK_\rho - iK_{-\rho\epsilon^*} \mid \mathfrak{R}_\rho \subseteq \mathfrak{J}\}$. To show $\mathfrak{A}$ is a real form of $\mathfrak{J}$ we only need to show it is closed under multiplication. If $x = \sum_\rho \lambda_\rho K_\rho \in \mathfrak{J}$, $\lambda_\rho \in \mathbf{C}$, we let $\bar{x} = \sum_\rho \bar{\lambda}_\rho K_\rho$. From the fact that the structure constants of $\mathfrak{J}$ with respect to the basis $\{K_\rho\}$ are real numbers (indeed, they are integers and half-integers, since $x \in \mathfrak{J}_{\mathbf{Z}}$ implies that $2R_x = U_{x,1}$ stabilizes $\mathfrak{J}_{\mathbf{Z}}$) it follows that

$$\overline{x \cdot y} = \bar{x} \cdot \bar{y}.$$

Since $K_\rho\sigma\epsilon = K_{-\rho\epsilon^*}$ whenever $K_\rho \notin R_{\mathfrak{J}}$, it is easy to see that $\mathfrak{A} = \{x \in \mathfrak{J} \mid \bar{x}\sigma\epsilon = x\}$. And if $x, y \in \mathfrak{A}$, then

$$(\overline{x \cdot y})\,\sigma\epsilon = (\bar{x} \cdot \bar{y})\,\sigma\epsilon = \bar{x}\sigma\epsilon \cdot \bar{y}\sigma\epsilon = x \cdot y.$$

To show that $\mathfrak{A}$ is compact we only need show that $t(\,,\,)$ is a real-valued positive definite form on $\mathfrak{A}$, i.e., that $t(x^{\cdot 2}) \geqslant 0$ for all $x \in \mathfrak{J}$ and $t(x^{\cdot 2}) = 0$ only if $x = 0$. We use Theorem 2 in the stronger form noted above: $t(K_\rho, K_{-\rho\epsilon^*}) = 1$ or 2. If $x = \sum \lambda_\rho K_\rho \in \mathfrak{A}$ then $x^{\cdot 2} = \sum_{\rho,\tau} \lambda_\rho\lambda_\tau K_\rho \cdot K_\tau$. Taking the trace of both sides, we get

$$t(x^{\cdot 2}) = \sum_\rho \lambda_\rho\bar{\lambda}_\rho t(K_\rho, K_{-\rho\epsilon^*}) = \sum_\rho |\lambda_\rho|^2 t(K_\rho, K_{-\rho\epsilon^*}).$$

Clearly $t(x^{\cdot 2}) \geqslant 0$ and $t(x^{\cdot 2}) = 0$ if and only if all $\lambda_\rho = 0$.

4. REDUCTION MODULO p

By $\mathbf{Z}$ we mean the ring of integers. We recall that $\mathfrak{R}_{\mathbf{Z}}$ is the additive abelian group generated by the chosen Chevalley basis of $\mathfrak{R}$ and that $\mathfrak{J}_{\mathbf{Z}} = \mathfrak{J} \cap \mathfrak{R}_{\mathbf{Z}}$

is the additive group generated by those basis elements lying in $\mathfrak{J}$. In general, if $\mathfrak{B}$ is any subspace of $\mathfrak{R}$ spanned by a subset of the basis, then by $\mathfrak{B}_{\mathbf{Z}}$ we mean the additive group generated by those basis elements lying in $\mathfrak{B}$. Let F be any field (usually we will assume that the characteristic of F is not 2). By $\mathfrak{R}_F$ we mean $\mathfrak{R}_{\mathbf{Z}} \otimes_{\mathbf{Z}} F$, and in general by $\mathfrak{B}_F$ we mean $\mathfrak{B}_{\mathbf{Z}} \otimes_{\mathbf{Z}} F$ (note that $\mathfrak{B}_F \subseteq \mathfrak{R}_F$). In the following we will have occasion to perform this construction with $\mathfrak{B} = \mathfrak{J}, \bar{\mathfrak{J}}, \mathfrak{L}, \mathfrak{H}, \mathfrak{J}_i, \mathfrak{R}_i$ $(=\mathfrak{R}(\mathfrak{J}_i)$, a direct summand of $\mathfrak{R}$).

$\mathfrak{J}_{\mathbf{Z}}$ is a subalgebra of $\mathfrak{J}$, regarded as a unital quadratic Jordan algebra over $\mathbf{Z}$ (see [3] for the relevant definitions). Hence $\mathfrak{J}_F$ is a unital quadratic Jordan algebra over F. If char $F \neq 2$ (which we henceforth assume), then $\mathfrak{J}_F$ has a natural structure as a (linear) Jordan algebra over F. The quadratic structure on $\mathfrak{J}_F$ is given as follows: If $a, b \in \mathfrak{J}_{\mathbf{Z}}$ and if $a \otimes 1$, $b \otimes 1$ denote the corresponding elements of $\mathfrak{J}_F$, then $(a \otimes 1)\, U_{b\otimes 1}$ is defined to be $aU_b \otimes 1$ [3, p. 1.9]. The linear structure is given by

$$R_{b\otimes 1} = \tfrac{1}{2}\,[U_{(b+1)\otimes 1} - U_{b\otimes 1} - U_{1\otimes 1}].$$

This may also be viewed as follows: If $a, b \in \mathfrak{J}_{\mathbf{Z}}$, then

$$\begin{aligned} 2(a \otimes 1) \cdot (b \otimes 1) &= (a \otimes 1)\,(U_{(b+1)\otimes 1} - U_{b\otimes 1} - U_{1\otimes 1}) \\ &= a(U_{b+1} - U_b - U_1) \otimes 1 = (2a \cdot b) \otimes 1. \end{aligned}$$

That is, $\mathfrak{J}_{\mathbf{Z}}$ is stabilized by U_b and $2R_b$, and the corresponding transformations on $\mathfrak{J}_F$ are $U_{b\otimes 1} = U_b \otimes 1$, $2R_{b\otimes 1} = (2R_b) \otimes 1$, where 1 here denotes the identity map.

Our first task is to obtain detailed information on the relationship between $\mathfrak{J}_F$ and $\mathfrak{R}_F$. First note that $\mathfrak{R}_{\mathbf{Z}} = \mathfrak{J}_{\mathbf{Z}} \oplus \bar{\mathfrak{J}}_{\mathbf{Z}} \oplus \mathfrak{L}_{\mathbf{Z}}$ and hence $\mathfrak{R}_F = \mathfrak{J}_F \oplus \bar{\mathfrak{J}}_F \oplus \mathfrak{L}_F$. Also $\mathfrak{J}_{\mathbf{Z}}\epsilon = \bar{\mathfrak{J}}_{\mathbf{Z}}$ (since $K_\rho\epsilon = \pm K_{\rho\epsilon^*}$), $\mathfrak{H}_{\mathbf{Z}}\epsilon = \mathfrak{H}_{\mathbf{Z}}$ (since $H_\rho\epsilon = \pm H_{\rho\epsilon^*}$), and $\mathfrak{L}_{\mathbf{Z}}\epsilon = \mathfrak{L}_{\mathbf{Z}}$. So ϵ stabilizes $\mathfrak{R}_{\mathbf{Z}}$ and $\epsilon \otimes 1$ is defined on $\mathfrak{R}_F$. By abuse of notation we will often write ϵ in place of $\epsilon \otimes 1$. Note that $\mathfrak{J}_F\epsilon = \bar{\mathfrak{J}}_F$, $\mathfrak{H}_F\epsilon = \mathfrak{H}_F$, and $\mathfrak{L}_F\epsilon = \mathfrak{L}_F$. Also $\epsilon^2 = 1$.

Assume for the moment that $\mathfrak{J}$ is simple. Then $\mathfrak{R}$ is simple. Let $\mathfrak{Z}$ be the center of $\mathfrak{R}_F$; by [7, 2.6], $\mathfrak{Z} = \{H \in \mathfrak{H}_F \mid [K_\rho \otimes 1, H] = 0 \text{ for all roots } \rho\}$ and $\mathfrak{R}_F/\mathfrak{Z}$ is simple, unless $\mathfrak{R}$ is of type G_2 and char $F = 3$. To show that these conclusions hold in all cases we show that $\mathfrak{R} \simeq G_2$ is impossible. Otherwise the simple system of roots of $\mathfrak{R}$ would be $\{\rho_1, \hat{\alpha}_1\}$ [2, p. 11], where either $2\rho_1 + 3\hat{\alpha}_1$ or $3\rho_1 + 2\hat{\alpha}_1$ is a root. But then we would have a root ρ such that $\rho(R_1) = 2$ or 3, a contradiction.

We claim that $\mathfrak{J}_F \oplus \bar{\mathfrak{J}}_F \oplus [\mathfrak{J}_F, \bar{\mathfrak{J}}_F] = \mathfrak{R}_F$. The left hand side $\mathfrak{U}$ is an ideal of $\mathfrak{R}_F$: for $[\mathfrak{J}_F, \mathfrak{L}_F] \subseteq \mathfrak{J}_F$, $[\bar{\mathfrak{J}}_F, \mathfrak{L}_F] \subseteq \bar{\mathfrak{J}}_F$, $[[\mathfrak{J}_F, \bar{\mathfrak{J}}_F], \mathfrak{L}_F] \subseteq [\mathfrak{J}_F, \bar{\mathfrak{J}}_F]$ by the Jacobi identity, and $[\mathfrak{J}_F, \mathfrak{J}_F] = [\bar{\mathfrak{J}}_F, \bar{\mathfrak{J}}_F] = 0$. $\mathfrak{U} + \mathfrak{Z}$ is therefore an ideal of $\mathfrak{R}_F$ containing $\mathfrak{Z}$. Since $\mathfrak{R}_F/\mathfrak{Z}$ is simple, $\mathfrak{U} + \mathfrak{Z} = \mathfrak{R}_F$. Now since

$\mathfrak{J}_F$, $\bar{\mathfrak{J}}_F$ are spanned by elements $K_\rho \otimes 1$, $[\mathfrak{J}_F, \bar{\mathfrak{J}}_F]$ is spanned by elements $[K_\rho, K_\tau] \otimes 1$ for suitable roots ρ, τ. So $\mathfrak{U}$ is the direct sum of certain spaces $\mathfrak{R}_\rho \otimes 1$ and some subspace of $\mathfrak{H}_F$. Since $\mathfrak{Z} \subseteq \mathfrak{H}_F$ and $\mathfrak{U} + \mathfrak{Z} = \mathfrak{R}_F$, we must have $K_\rho \otimes 1 \in \mathfrak{U}$ for all roots ρ of $\mathfrak{R}$. It follows that

$$H_\rho \otimes 1 = [K_\rho \otimes 1, K_{-\rho} \otimes 1] \in [\mathfrak{U}, \mathfrak{U}] \subseteq \mathfrak{U}$$

for all roots ρ, hence that $\mathfrak{H}_F \subseteq \mathfrak{U}$. We conclude that $\mathfrak{U} = \mathfrak{R}_F$.

If $\mathfrak{J}$ isn't simple, say $\mathfrak{J} = \oplus \sum_i \mathfrak{J}_i$ (where $\mathfrak{J}_i$ are simple ideals of $\mathfrak{J}$), then $\mathfrak{R} = \oplus \sum_i \mathfrak{R}_i$, where $\mathfrak{R}_i \simeq \mathfrak{R}(\mathfrak{J}_i)$; and $\mathfrak{R}_{\mathbf{Z}} = \oplus \sum_i \mathfrak{R}_{i\mathbf{Z}}$, hence $\mathfrak{R}_F = \oplus \sum_i \mathfrak{R}_{iF}$. If $\mathfrak{Z}_i$ is the center of $\mathfrak{R}_{iF}$ then $\mathfrak{Z} = \oplus \sum_i \mathfrak{Z}_i$ is the center of $\mathfrak{R}_F$. We apply the above discussion to the simple components of $\mathfrak{J}$ and conclude that

$$\begin{aligned}\mathfrak{J}_F \oplus \bar{\mathfrak{J}}_F \oplus [\mathfrak{J}_F, \bar{\mathfrak{J}}_F] &= \oplus \sum_i \mathfrak{J}_{iF} \oplus \bar{\mathfrak{J}}_{iF} \oplus [\mathfrak{J}_{iF}, \bar{\mathfrak{J}}_{iF}] \\ &= \oplus \sum_i \mathfrak{R}_{iF} = \mathfrak{R}_F\end{aligned}$$

and that $\mathfrak{R}_F/\mathfrak{Z} \simeq \oplus \sum_i \mathfrak{R}_{iF}/\mathfrak{Z}_i$ is a direct sum of simple ideals, hence is semisimple.

LEMMA 8. (a) *If* $L \in \mathfrak{L}_F$ *then* $L\epsilon = L$ *if and only if* $[1, L] = 0$.

(b) $\mathfrak{Z} = \{L \in \mathfrak{L}_F \mid [\mathfrak{J}_F, L] = 0\}$.

Proof. (a) If $L \in \mathfrak{L}$ then $[1, L + L\epsilon] = 0$ and $[[1, L - L\epsilon], \bar{1}] = 2(L - L\epsilon)$. This is because $L + L\epsilon$ is fixed by ϵ, so belongs to $\mathfrak{D}$, whereas $L - L\epsilon$ (which is mapped to its negative by ϵ) must belong to $R_{\mathfrak{J}}$. If $L \in \mathfrak{L}_{\mathbf{Z}}$, these formulas remain true and can be interpreted to hold in $\mathfrak{R}_F$ (i.e., they hold if we replace L by $L \otimes 1$, 1 by $1 \otimes 1$, ϵ by $\epsilon \otimes 1$, etc.). Since $\mathfrak{L}_{\mathbf{Z}} \otimes 1$ spans $\mathfrak{L}_F$, these formulas hold for all $L \in \mathfrak{L}_F$.

If $L\epsilon = L$, then $[1, L] = [1, \frac{1}{2}(L + L\epsilon)] = 0$.

If $[1, L] = 0$, then

$$0 = [[1, L], \bar{1}] = [[1, \tfrac{1}{2}(L - L\epsilon) + \tfrac{1}{2}(L + L\epsilon)], \bar{1}] = L - L\epsilon + 0.$$

So $L = L\epsilon$.

(b) Since $\mathfrak{Z} \subseteq \mathfrak{H}_F \subseteq \mathfrak{L}_F$, clearly $\mathfrak{Z} \subseteq \{L \mid [\mathfrak{J}_F, L] = 0\}$. If $[\mathfrak{J}_F, L] = 0$, then $[1, L] = 0$ and hence $L\epsilon = L$ by (a). So

$$[\bar{\mathfrak{J}}_F, L] = [\mathfrak{J}_F\epsilon, L\epsilon] = [\mathfrak{J}_F, L]\epsilon = 0.$$

This certainly implies that $[[\mathfrak{J}_F, \bar{\mathfrak{J}}_F], L] = 0$ and thus that $[\mathfrak{R}_F, L] = 0$. We conclude that $L \in \mathfrak{Z}$. This completes the proof.

The formula $[c[a\bar{b}]] = b(U_{a+c} - U_a - U_c)$ holds for $a, b, c \in \mathfrak{J}_Z$, hence for $a, b, c \in \mathfrak{J}_Z \otimes 1$. Since both sides are linear in a, b, c, it holds for all $a, b, c \in \mathfrak{J}_F$. Note also that

$$b(U_{a+c} - U_a - U_c) = bU_{a,c} = c(2R_{a\cdot b} - 2[R_a, R_b])$$

by [5, p. 325].

THEOREM 3. *$\mathfrak{R}_F/\mathfrak{Z}$ is isomorphic to $\mathfrak{R}(\mathfrak{J}_F)$, the Koecher–Tits algebra of $\mathfrak{J}_F$.*

Proof. If $L \in \mathfrak{L}_F$, let L' be the linear transformation of $\mathfrak{J}_F$ defined by $a \mapsto [a, L]$. $L' \in \mathfrak{L}(\mathfrak{J}_F)$; this is certainly true if $L = [b, \bar{c}]$ since, as we have seen, $[a[b\bar{c}]] = a(2R_{b\cdot c} - 2[R_b, R_c])$. It holds for all $L \in \mathfrak{L}_F$ since $\mathfrak{L}_F$ is spanned by elements of the form $[b, \bar{c}]$.

We show that $(L\epsilon)' = L'\epsilon$ (here the letter ϵ is used in two senses: the transformation $\epsilon \otimes 1$ of $\mathfrak{L}_F$, and the usual involution on $\mathfrak{L}(\mathfrak{J}_F)$). This holds for $L = [b, \bar{c}]$ since

$$\begin{aligned} ([b, \bar{c}]\,\epsilon)' &= [\bar{b}, c]' = -[c, \bar{b}]' = -(2R_{c\cdot b} - 2[R_c, R_b]) \\ &= -2R_{b\cdot c} - 2[R_b, R_c] = [b, \bar{c}]'\,\epsilon. \end{aligned}$$

It holds for general L by linearity.

$L \mapsto L'$ is onto $\mathfrak{L}(\mathfrak{J}_F) : [a\,[\tfrac{1}{2}\,b, \bar{1}]] = aR_b$ and $\mathfrak{L}(\mathfrak{J}_F)$ is generated by $\{R_b \mid b \in \mathfrak{J}_F\}$. The mapping $L \to L'$ is a homomorphism of Lie algebras, since for $L_1, L_2 \in \mathfrak{L}_F$ the Jacobi identity gives $[a[L_1L_2]] = [[aL_1]\,L_2] - [[aL_2]\,L_1]$. Finally, the kernel of this homomorphism is $\mathfrak{Z}$ by Lemma 8(b).

If $K = a + \bar{b} + L \in \mathfrak{R}_F\,(a \in \mathfrak{J}_F,\ \bar{b} \in \bar{\mathfrak{J}}_F,\ L \in \mathfrak{L}_F)$, we let $K' = a + \bar{b} + L' \in \mathfrak{J}_F \oplus \bar{\mathfrak{J}}_F \oplus \mathfrak{L}(\mathfrak{J}_F) = \mathfrak{R}(\mathfrak{J}_F)$. Then $K \to K'$ is a homomorphism from $\mathfrak{R}_F$ to $\mathfrak{R}(\mathfrak{J}_F)$; it is clearly linear, and it preserves multiplication because of the following: If $a, b \in \mathfrak{J}_F$, $L_1, L_2, L_3 \in \mathfrak{L}_F$, then

$$\begin{aligned} &[L_1', L_2'] = [L_1, L_2]', \\ &\quad [a, \bar{b}]' = 2R_{a\cdot b} - 2[R_a, R_b] = [a', \bar{b}'], \\ &\quad [a, L]' = [a, L] = aL' = [a', L'], \\ &\quad [\bar{a}, L]' = [\bar{a}, L] = [a\epsilon, L] = [a, L\epsilon]\,\epsilon \\ &\qquad = (a(L\epsilon)')\,\epsilon = (a(L'\epsilon))\,\epsilon \\ &\qquad = [a', L'\epsilon]\,\epsilon = [\bar{a}', L'], \\ &[\mathfrak{J}_F, \mathfrak{J}_F] = [\bar{\mathfrak{J}}_F, \bar{\mathfrak{J}}_F] = 0 \text{ in both } \mathfrak{R}_F \text{ and } \mathfrak{R}(\mathfrak{J}_F). \end{aligned}$$

Since $L \mapsto L'$ is onto $\mathfrak{L}(\mathfrak{J}_F)$, $K \mapsto K'$ is clearly onto $\mathfrak{R}(\mathfrak{J}_F)$. The kernel of $K \mapsto K'$ is clearly $\mathfrak{Z}$; so $\mathfrak{R}_F/\mathfrak{Z} \cong \mathfrak{R}(\mathfrak{J}_F)$.

COROLLARY. *$\mathfrak{J}_F$ is semisimple and is simple if and only if $\mathfrak{J}$ is simple.*

Proof. We have seen that $\mathfrak{R}_F/\mathfrak{Z}$ is semisimple and is simple if and only if $\mathfrak{J}$ is simple. The semisimplicity of $\mathfrak{R}(\mathfrak{J}_F)$ implies that of $\mathfrak{J}_F$ [5, p. 333]. Also, $\mathfrak{J}$ is simple if and only if $\mathfrak{R}(\mathfrak{J}_F)$ is, i.e., if and only if $\mathfrak{J}_F$ is.

We now study some idempotents of $\mathfrak{J}_F$. If $e \in \mathfrak{J}_{\mathbf{Z}}$ is an idempotent then clearly $e \otimes 1 \in \mathfrak{J}_F$ is also an idempotent. $2R_e$ is a linear transformation of $\mathfrak{J}$ which leaves $\mathfrak{J}_{\mathbf{Z}}$ invariant, so that its matrix with respect to the basis $\{K_\rho\}$ of $\mathfrak{J}$ has integral entries. Since $(2R_e) \otimes 1 = 2R_{e\otimes 1}$, the matrix of $2R_{e\otimes 1}$ with respect to the basis $\{K_\rho \otimes 1\}$ of $\mathfrak{J}_F$ is the same as the matrix of $2R_e$, except that the entries are interpreted as belonging to F instead of Φ. $2R_e$ is a diagonalizable linear transformation with eigenvalues 1, 2, 0 so that the characteristic polynomial of $2R_e$ is $(\lambda - 1)^i (\lambda - 2)^j \lambda^k$; here $i = \dim \mathfrak{J}_{1/2}(e)$, $j = \dim \mathfrak{J}_1(e)$, $k = \dim \mathfrak{J}_0(e)$. Clearly, this is also the characteristic polynomial of $2R_{e\otimes 1}$ (in which 1 and 2 are elements of F). We conclude that the dimensions of the Peirce spaces of e in $\mathfrak{J}$ are the same as the dimensions of the corresponding Peirce spaces of $e \otimes 1$ in $\mathfrak{J}_F$. This applies, in particular, to the idempotents e_ρ $(\rho \in P)$. Note that by the Corollary to Lemma 5, e_ρ is primitive if and only if $\dim \mathfrak{J}_1(e_\rho) = 1$. So e_ρ primitive implies that $e_\rho \otimes 1$ is primitive.

Suppose that $\rho \in P$ is such that e_ρ is not primitive; let $\tau \neq \rho$ be such that $K_\tau \in \mathfrak{J}_{\rho\rho}$ and let $x = K_\tau$, $y = K_{-\tau\epsilon^*}$, $x \cdot y = (s/2)\, e_\rho$ (as in Lemma 5). Let $a = e_\rho + x + sy$ and $b = e_\rho - x - sy$, so that $e_\rho = \frac{1}{2}a + \frac{1}{2}b$ is a decomposition of e_ρ as a sum of orthogonal primitive idempotents. Note that $a, b \in \mathfrak{J}_{\mathbf{Z}}$. Now $a^{\cdot 2} = 2a$ and $b^{\cdot 2} = 2b$, so that $(a \otimes 1)^{\cdot 2} = 2a \otimes 1$ and $(b \otimes 1)^{\cdot 2} = 2b \otimes 1$. This implies that $\frac{1}{2}a \otimes 1$ and $\frac{1}{2}b \otimes 1$ are idempotents in $\mathfrak{J}_F$ (whose sum is $e_\rho \otimes 1$). $R_{\frac{1}{2}a} = \frac{1}{2}R_a$ is a diagonalizable linear transformation of $\mathfrak{J}$ with eigenvalues $\frac{1}{2}$, 1, 0, so that $2R_a$ is a diagonalizable linear transformation of $\mathfrak{J}$ which leaves $\mathfrak{J}_{\mathbf{Z}}$ invariant and has eigenvalues 2, 4, 0. If its characteristic polynomial is $(\lambda - 2)^i (\lambda - 4)^j \lambda^k$, then, as before, $2R_{a\otimes 1}$ has the same characteristic polynomial. Since $j = 1$, by the proof of Lemma 5, $\frac{1}{2}a \otimes 1$ must be primitive. Also the Peirce $\frac{1}{2}$-spaces of $\frac{1}{2}a$ (in $\mathfrak{J}$) and $\frac{1}{2}a \otimes 1$ (in $\mathfrak{J}_F$) have the same dimensions.

If $x, y \in \mathfrak{J}$ and $x \cdot y = 0$, clearly $(x \otimes 1) \cdot (y \otimes 1) = 0$ in $\mathfrak{J}_F$. Applying this to the above, we see that we have written the identity of $\mathfrak{J}_F$ as a sum of primitive orthogonal idempotents. These idempotents are in correspondence with the elements of a complete orthogonal set of idempotents of $\mathfrak{J}$ in such a way that the dimensions of the $\frac{1}{2}$-spaces of corresponding idempotents are the same.

The proof of the following theorem uses these considerations and also depends on the classification theory of simple Jordan algebras.

THEOREM 4. *If F is algebraically closed, then every semisimple Jordan algebra over F is of the form $\mathfrak{J}_F$ for some semisimple Jordan algebra $\mathfrak{J}$ over Φ.*

Proof. By taking direct sums one can easily see that it is sufficient to prove this theorem for simple Jordan algebras over F. Finite-dimensional simple Jordan algebras over an algebraically closed field are classified by two integers: the cardinality n of a complete set of orthogonal primitive idempotents, and the dimension d of the Peirce half-spaces $\mathfrak{J}_{1/2}(e) \cap \mathfrak{J}_{1/2}(f)$, where e, f are orthogonal primitive idempotents. The possibilities are: $n = 1$, $d = 0$; $n = 2$, $d \geqslant 1$; $n = 3$, $d = 1, 2, 4, 8$; $n \geqslant 4$, $d = 1, 2, 4$ [5, Chapter V]. Since the dimension of $\mathfrak{J}_{1/2}(e)$ (where e is a primitive idempotent) is $(n - 1)\, d$, we see that the simple algebras are also classified by the integers n and dim $\mathfrak{J}_{1/2}(e)$.

The above discussion about idempotents shows that the cardinality of complete sets of orthogonal primitive idempotents of $\mathfrak{J}$ and $\mathfrak{J}_F$ are the same, and also that the dimensions of the half-spaces of primitive idempotents are the same for $\mathfrak{J}$ and $\mathfrak{J}_F$. Since $\mathfrak{J}_F$ is simple when $\mathfrak{J}$ is, we can get $\mathfrak{J}_F$ to be the simple algebra over F characterized by two integers n, d by choosing $\mathfrak{J}$ to be the simple algebra over Φ characterized by the same two integers. This completes the proof.

We can use Theorem 2 to give an alternate proof of the fact that $\mathfrak{J}_F$ is semisimple. First we will compare the generic minimum polynomials of $\mathfrak{J}$ and $\mathfrak{J}_F$. We follow the discussion in [5, pp. 221–229]. For each root ρ such that $\mathfrak{K}_\rho \subseteq \mathfrak{J}$, let ξ_ρ be an indeterminant. If R is a ring, $R[\xi]$ will be the ring of all polynomials in $\{\xi_\rho\}$ over R; if F is a field, $F(\xi)$ will be the field of all rational functions in $\{\xi_\rho\}$ over F. Let X be the generic element $\sum_\rho \xi_\rho \cdot 2K_\rho$ of $\mathfrak{J}$. The minimum polynomial of X in $\mathfrak{J}_{\Phi(\xi)}$ is the generic minimum polynomial of $\mathfrak{J}$, which we write as

$$m_X(\lambda) = \lambda^m - \sigma_1(\xi)\, \lambda^{m-1} + \sigma_2(\xi)\, \lambda^{m-2} - \cdots + (-1)^m\, \sigma_m(\xi).$$

Here $\sigma_i(\xi) \in \Phi(\xi)$.

LEMMA 9. *$\sigma_i(\xi) \in \mathbf{Z}[\xi]$ for $i = 1, \ldots, m$.*

Proof. Certainly $\sigma_i(\xi) \in \mathbf{Q}(\xi)$, where $\mathbf{Q}$ is the field of rational numbers. For $X \in \mathfrak{J}_{\mathbf{Q}(\xi)} \subseteq \mathfrak{J}_{\Phi(\xi)}$, hence all $X^i \in \mathfrak{J}_{\mathbf{Q}(\xi)}$. And if $1, X, \ldots, X^{m-1}$ are those powers of X which are linearly independent over $\mathbf{Q}(\xi)$, they are also linearly independent over $\Phi(\xi)$ (since $\mathfrak{J}_{\Phi(\xi)} = \mathfrak{J}_{\mathbf{Q}(\xi)} \otimes \Phi(\xi)$).

We apply the argument of [5, p. 222]. Let $f(\lambda)$ be the characteristic polynomial of the linear transformation R_X. Since $X = 2 \sum_\rho \xi_\rho K_\rho$, R_X stabilizes $\mathfrak{J}_{\mathbf{Z}[\xi]}$, the set of all linear combinations of $\{K_\rho\}$ with coefficients in $\mathbf{Z}[\xi]$. Hence the matrix of R_X has entries in $\mathbf{Z}[\xi]$, and $f(\lambda)$ is a monic polynomial with coefficients in $\mathbf{Z}[\xi]$. Since $m_X(\lambda)$ divides $f(\lambda)$ [5, p. 221], and since the field of quotients of $\mathbf{Z}[\xi]$ is $\mathbf{Q}(\xi)$, we conclude from Gauss's Lemma that the coefficients of $m_X(\lambda)$ are in $\mathbf{Z}[\xi]$. This completes the proof.

Note that $\mathbf{Z}[\xi] \otimes_{\mathbf{Z}} F = F[\xi]$. If $\theta \in \mathbf{Z}[\xi]$, then $\theta \otimes 1$ is that element of $F[\xi]$ obtained by interpreting the coefficients of θ as elements of F. Note also that $\mathfrak{J}_{\mathbf{Z}[\xi]} \otimes_{\mathbf{Z}} F = \mathfrak{J}_{F[\xi]}$, so that $X \otimes 1 \in \mathfrak{J}_{F[\xi]}$. $X \otimes 1 = \sum_\rho \xi_\rho \cdot 2K_\rho \otimes 1$, so that $X \otimes 1$ is a generic element of $\mathfrak{J}_F$.

THEOREM 5. *The generic minimum polynomial of* $\mathfrak{J}_F$ *(more precisely, the minimum polynomial of* $X \otimes 1$ *in* $\mathfrak{J}_{F(\xi)}$*) is*

$$m_{X\otimes 1}(\lambda) = \lambda^m - (\sigma_1 \otimes 1)(\xi)\lambda^{m-1} + (\sigma_2 \otimes 1)(\xi)\lambda^{m-2} - \cdots + (-1)^m (\sigma_m \otimes 1)(\xi).$$

Proof. We first show that $X \otimes 1$ satisfies the above polynomial. In the equation $X^m - \sigma_1(\xi) X^{m-1} + \cdots + (-1)^m \sigma_m(\xi) 1 = 0$ we tensor both sides of the equation with 1 and get

$$(X \otimes 1)^m - (\sigma_1 \otimes 1)(\xi)(X \otimes 1)^{m-1} + \cdots + (-1)^m (\sigma_m \otimes 1)(\xi) 1 = 0$$

as desired. Note that all powers of X belong to $\mathfrak{J}_{\mathbf{Z}[\xi]}$ since $\mathfrak{J}_{\mathbf{Z}[\xi]}$ is a quadratic Jordan algebra, and that $X^k \otimes 1 = (X \otimes 1)^k$ by induction, since $(X^k U_X) \otimes 1 = (X^k \otimes 1)(U_X \otimes 1)$.

So the minimum polynomial of $X \otimes 1$ divides the above polynomial. We show the two polynomials have the same degree. Now σ_1 is the generic trace of $\mathfrak{J}$, and $m = \sigma_1(1)$ (1 is here the identity of $\mathfrak{J}$). Since 1 is the sum of primitive orthogonal idempotents which have trace 1, there must be m elements in this complete set of idempotents. Our computations with idempotents show that the identity of $\mathfrak{J}_F$ is a sum of the same number m of primitive idempotents. Hence by [5, p. 229, Lemma 1] the degree of the generic minimum polynomial of $\mathfrak{J}_F$ is at least m. Since it is also at most m, it must be exactly m. This completes the proof.

COROLLARY 1. *If t is the generic trace of $\mathfrak{J}$ and t_F the generic trace of $\mathfrak{J}_F$, then there exist integers n_ρ (for all roots ρ such that $\mathfrak{R}_\rho \subseteq \mathfrak{J}$) satisfying*

$$2t\left(\sum_\rho \xi_\rho K_\rho\right) = \sum_\rho n_\rho \xi_\rho \qquad \textit{for all } \xi_\rho \in \Phi,$$

$$2t_F\left(\sum_\rho \xi_\rho K_\rho \otimes 1\right) = \sum_\rho n_\rho \xi_\rho \qquad \textit{for all } \xi_\rho \in F.$$

Proof. Since σ_1 belongs to $Z[\xi]$ and has degree one, it must be of the form $\sigma_1(\xi) = \sum_\rho n_\rho \xi_\rho$ for some integers n_ρ. But

$$\sigma_1(\xi) = t(X) = t\left(\sum_\rho \xi_\rho \cdot 2K_\rho\right) = 2t\left(\sum_\rho \xi_\rho K_\rho\right).$$

Specializing the indeterminants ξ_ρ to elements of Φ, we obtain the first equation. Now Theorem 5 says that $\sigma_1 \otimes 1$ is the generic trace of $\mathfrak{J}_F$, i.e., that $2t_F(\sum_\rho \xi_\rho K_\rho \otimes 1) = t_F(X \otimes 1) = (\sigma_1 \otimes 1)(\xi) = \sum_\rho n_\rho \xi_\rho$. If we specialize the ξ_ρ to elements of F, we obtain the second formula.

COROLLARY 2. *The generic trace bilinear form $t_F(\,,\,)$ of $\mathfrak{J}_F$ is nondegenerate. $\mathfrak{J}_F$ is semisimple.*

Proof. By Corollary 1, if $x \in \mathfrak{J}_{\mathbf{Z}}$, then $2t(x)$ is an integer and $2t_F(x \otimes 1)$ is the same integer (regarded as an element of F). Hence if ρ, τ are two roots such that $\mathfrak{R}_\rho, \mathfrak{R}_\tau \subseteq \mathfrak{J}$, then $2t(2K_\rho \cdot K_\tau)$ is an integer and $2t_F(2(K_\rho \otimes 1) \cdot (K_\tau \otimes 1))$ is the same integer. Theorem 2 tells what this integer is: It is zero unless $\tau = -\rho\epsilon^*$, in which case it is ± 4, ± 8. So the determinant of the matrix of $4t_F(\,,\,)$ with respect to the basis $\{K_\rho \otimes 1\}$ of $\mathfrak{J}_F$ is plus or minus a power of 2, hence is nonzero. So $4t_F(\,,\,)$ is a nondegenerate form, as then is $t_F(\,,\,)$.

That $\mathfrak{J}_F$ is semisimple now follows from [5, p. 240, Theorem 5].

REFERENCES

1. C. CHEVALLEY, Sur certains groupes simples, *Tôhoku Math. J.* **7** (1956), 14–66.
2. S. R. GORDON, The components of the automorphism group of a Jordan algebra, *Trans. Amer. Math. Soc.* **153** (1971), 1–52.
3. N. JACOBSON, "Lectures on Quadratic Jordan Algebras," Tata Institute of Fundamental Research, Bombay, 1969.
4. N. JACOBSON, "Lie Algebras," Interscience, New York, 1962.
5. N. JACOBSON, "Structure and Representations of Jordan Algebras," Amer. Math. Soc. Colloq. Publ., Vol. 39, American Mathematical Society, Providence, RI, 1968.
6. M. KNEBUSCH, Der Begriff der Ordnung einer Jordanalgebra, *Abh. Math. Sem. Univ. Hamburg* **28** (1965), 168–184.
7. R. STEINBERG, Automorphisms of classical Lie algebras, *Pacific J. Math.* **11** (1961), 1119–1129.
8. R. STEINBERG, "Lectures on Chevalley Groups," mimeographed notes, Yale University, New Haven, CT, 1967.